



FFI Forsvarets
forskningsinstitutt

26/013

FFI-RAPPORT

Posisjon, navigasjon og tid

– og betydningen for totalforsvaret

Lily Hübert
Tor Atle Solend
Anders Rødningsby
Stig Rune Sellevåg

Posisjon, navigasjon og tid

– og betydningen for totalforsvaret

Lily Hübert
Tor Atle Solend
Anders Rødningsby
Stig Rune Sellevåg

Emneord

PNT (posisjon, navigasjon og tid)

GNSS

Totalforsvar

Romteknologi

FFI-rapport

26/013

Prosjektnummer

6177

Online ISSN

2704-2383

Engelsk tittel

Position, navigation and time – and its impact for total defence

Godkjennere

Stig Rune Sellevåg, *forskningsleder*

Tonje Nanette Arnesen, *forskningsleder*

Janet Martha Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Opphavsrett

© Forsvarets forskningsinstitutt (FFI). Publikasjonen kan siteres fritt med kildehenvisning.

Sammendrag

På oppdrag fra Nærings- og fiskeridepartementet har Forsvarets forskningsinstitutt vurdert betydningen satellittbasert posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT) har for totalforsvaret. Globale navigasjonssatellittsystemer (GNSS) har i økende grad blitt integrert i flere deler av samfunnet som en kilde til svært nøyaktig posisjon og tid. Samtidig er GNSS-signalene svake og svært sårbare for elektromagnetiske forstyrrelser, både naturlige og menneskeskapte. Slike forstyrrelser har funnet sted i Norge de siste årene, og Etterretningstjenesten vurderer i den åpne trusselvurderingen at verdensrommet kan være en fremtidig arena for krigføring.

Hovedfokuset i rapporten er en vurdering av GNSS-avhengigheter, men romvirksomhet i stort er også diskutert. I denne studien kartlegger vi ulike bruksområder av GNSS i samfunnet og beskriver tilskitende handlinger og farer som kan føre til bortfall av GNSS og andre satellitt-tjenester. Deretter vurderer vi betydningen GNSS har for totalforsvarsevnen basert på en risikoanalyse for kritiske samfunnsfunksjoner. Studien har identifisert sektorovergrepende sårbarheter som øker risiko for totalforsvaret. Disse inkluderer den økende avhengigheten til GNSS og flere usikkerhetsmomenter knyttet til hvorvidt samfunnsfunksjoner kan motstå forstyrrelser i GNSS.

Vi vurderer at satellittbasert PNT styrker totalforsvaret, og at GNSS-forstyrrelser vil redusere effektivitet og kapasitet i flere kritiske samfunnsfunksjoner sammenlignet med dagens tilstand. Bruk av feil tidsdata, som følge av stadig mer avanserte spoofing-angrep, øker risiko for tap av funksjonsevne, særlig i digitale og automatiserte systemer. Mangel eller feil på GNSS-signaler vil øke faren for tap av liv og helse, særlig knyttet til nødetatenes behov for PNT, og redusere situasjonsbevissthet i hele krisespekteret. Dette kan blant annet føre til farlige situasjoner for transporttjenester og forsinkelser i leveranser av forsyninger. GNSS-forstyrrelser kan skape problemer for kraftforsyningen og mobilnettet.

Vi anbefaler seks risikoreduserende tiltak som vil øke PNT-motstandsdyktigheten i Norge:

- tilrettelegge for og gjennomføre testing av utstyr for å identifisere og kartlegge sårbarheter
- utvikle nasjonale rammeverk og retningslinjer for PNT og krav til samfunnssektorer for redundans
- utvikle bakkebaserte alternativer for å ivareta en stabil tidsreferanse i Norge og Norges økonomiske sone
- gjøre bruken av GNSS mer motstandsdyktig
- utvikle robuste multi-sensor PNT-systemer
- fortsette med internasjonalt samarbeid for å forbedre sikkerheten og tilgjengeligheten av satellittbasert PNT og andre satellitt-tjenester

Summary

Commissioned by the Ministry of Trade, Industry and Fisheries, the Norwegian Defence Research Establishment (FFI) has assessed the importance of satellite-based position, navigation, and time (PNT) for Norway's total defense. Global navigation satellite systems (GNSS) have increasingly been integrated into several parts of society as a source for highly accurate position and time. However, GNSS signals are very weak and highly vulnerable to electromagnetic disturbances, both natural and manmade. Norway has increasingly experienced such disturbances, and in their open threat assessment The Norwegian Intelligence Service assessed how outer space can be a future arena for warfighting.

The main focus of our report is to assess GNSS, although other parts of the space industry are also discussed. The study has mapped different uses of GNSS in society and described intentional actions and hazards that can lead to loss of GNSS services and other satellite services. We have assessed the importance of GNSS for Norway's total defense capability based on a risk analysis of critical societal functions. Our study has also identified several cross-sectoral vulnerabilities that increase the risk for total defense, including an increased dependency on GNSS and several uncertainty elements related to the ability of societal functions to withstand GNSS disturbances.

We have concluded that satellite-based PNT strengthens Norway's total defense and that loss of GNSS will reduce functional capabilities. The use of incorrect position or time data as a result of increasingly advanced spoofing attacks increases the risk for loss of functional capability in several societal functions. Loss of GNSS services increases the possibility for loss of life and health, especially relating to the emergency services' need for PNT, and reduces situational awareness in the entire crisis spectrum. This may, for example, create dangerous situations for transport services and delays in supply deliveries. GNSS disturbances can cause problems for electricity supply and mobile networks.

We recommend six measures that will reduce risk and increase PNT resilience in Norway:

- enabling and conducting testing of equipment to identify and map vulnerabilities
- developing national frameworks and standards for PNT that include requirements for societal sectors
- developing ground-based alternatives to maintain and secure a stable time reference in Norway and Norway's economic zone
- ensuring more resilient use of GNSS
- developing robust multi-sensor PNT systems
- continuing international collaboration to improve the security and availability of satellite based PNT and satellite service

Innhold

Sammendrag	3
Summary	4
Forord	7
Forkortelser	8
1 Innledning	9
1.1 Formål og avgrensninger	10
1.2 Rapportens struktur	11
2 Totalforsvar og PNT	12
3 PNT og satellittbaserte tjenester i Norge	14
3.1 Romvirksomhet	14
3.1.1 Globale navigasjonssatellittsystemer – GNSS	14
3.1.2 Andre satellittbaserte tjenester	15
3.2 Tidsbestemmelse	16
3.2.1 Kartlagte bruksområder for tidsbestemmelse	20
3.3 Posisjonsbestemmelse	24
3.3.1 Kartlagte bruksområder for posisjonsbestemmelse	26
4 Trusler og farer mot GNSS	30
4.1 Radiofrekvensinterferens – RFI	30
4.1.1 RFI mot geostasjonære satellitter og lavbanesatellitter	34
4.1.2 RFI fra satellitter	34
4.1.3 Sårbarhet i beskyttelsestiltak mot RFI	35
4.2 Cyberangrep	35
4.3 Ødeleggelse av fysisk infrastruktur	36
4.4 Bortfall av GNSS i hele krisespekteret	37
4.4.1 Lokale forstyrrelser av GNSS	37
4.4.2 Omfattende bortfall av GNSS	38
5 Hvilken risiko medfører GNSS-forstyrrelser for totalforsvaret?	39

5.1	Vurdering av sårbarheter og konsekvenser	40
5.1.1	Kraftforsyning	40
5.1.2	Olje- og gassnæringen og drivstofforsyning	42
5.1.3	Ekomtjenester	44
5.1.4	Vannforsyning	45
5.1.5	Betalingssystemer	46
5.1.6	Sjøtransport	47
5.1.7	Veitransport	51
5.1.8	Jernbanetransport	52
5.1.9	Lufttransport	53
5.1.10	Matdistribusjon	55
5.1.11	Nødetater	57
5.2	Oppsummering og diskusjon	58
5.2.1	Sektorovergripende funn	58
5.2.2	Risiko for totalforsvarsevne	59
6	Risikoreduserende tiltak	64
7	Konklusjon	68
	Vedlegg	70
A	Metodisk tilnærming	70
A.1	Avgrensninger	70
A.2	Datainnsamling	70
A.3	Kriterier for risikoanalyse	77
B	Alternativ og fremtidig PNT-teknologi	79
B.1	LEO PNT	79
B.2	Kvanteteknologi	80
B.3	Sekundærbruk av signaler (signals of opportunity)	80
B.4	eLoran	81
B.5	White Rabbit	81
C	Oppsummering av tiltak diskutert av fageksperter	82
	Referanser	84

Forord

FFI har på oppdrag fra Nærings- og fiskeridepartementet (NFD) vurdert betydningen satellittbasert PNT for totalforsvaret. Oppdraget ble utført i perioden våren 2025 til våren 2026. Dette arbeidet bidrar til kunnskapsgrunnlaget om PNT i Norge for å styrke evnen til å motstå forstyrrelser. Arbeidet har skjedd parallelt med en samfunnsøkonomisk analyse av satellittbasert PNT gjennomført av Menon Economics og en analyse av krisescenarioer utarbeidet av Direktoratet for samfunnssikkerhet og beredskap (DSB). Vi vil gjerne takke alle som har deltatt på intervjuer og diskusjoner og bidratt med kunnskap, korrekturlesing og innspill underveis.

Kjeller, 19. mai 2026

Lily Hübert, Tor Atle Solend, Anders Rødningsby, Stig Rune Sellevåg

Forkortelser

PNT	Posisjonsbestemmelse, Navigasjon og Tidsbestemmelse
GPS	Global Positioning System
GNSS	Global Navigation Satellite Systems
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
GEO	Geostationary Earth Orbit
GBAS	Ground-Based Augmentation Systems
SBAS	Satellite-Based Augmentation Systems
EGNOS	European Geostationary Navigation Overlay Service
ESA	European Space Agency
AIS	Automatisk Identifikasjonssystem
UTC	Universal Coordinated Time
NTP	Network Time Protocol
PTP	Precision Time Protocol
IoT	Internet of Things
SCADA	Supervisory Control and Data Acquisition
DP	Dynamisk Posisjonering
PBN	Performance-Based Navigation

1 Innledning

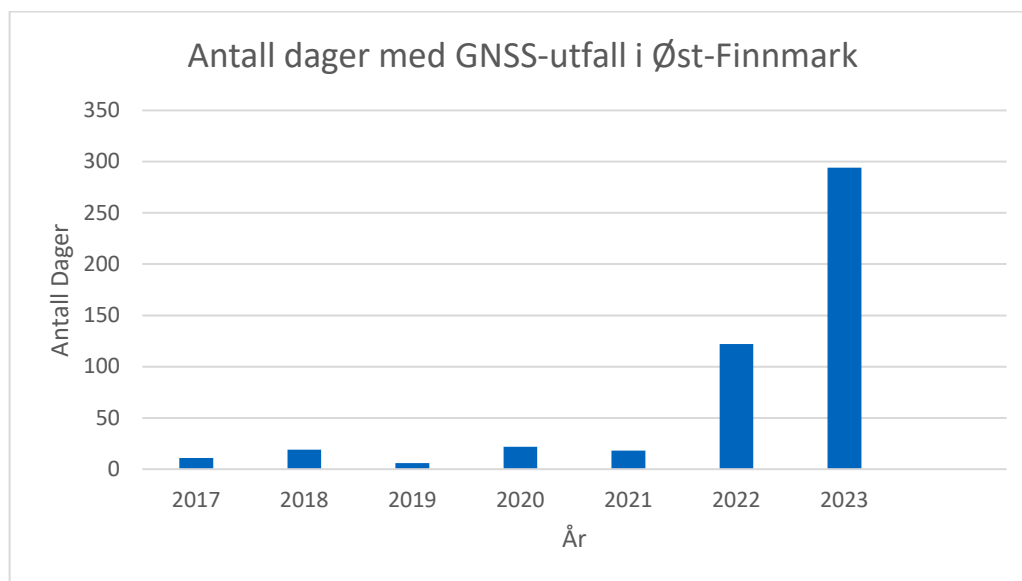
I år 2000 fikk det globale samfunnet tilgang til svært presis posisjon. Dette var et resultat av at den nøyaktige posisjonstjenesten til GPS (*Global Positioning System*) ble gjort tilgjengelig for sivilsamfunnet. Siden da har satellittbasert posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT), gjennom GNSS (globale navigasjonssatellittsystemer), blitt en integrert del av samfunnet. Samtidig blir tilgjengeligheten og nøyaktigheten stadig bedre med flere og nyere satellitter og både bakke- og rombaserte støttesystemer.

Den åpne risikovurderingen til Nasjonal sikkerhetsmyndighet (NSM) fra 2025 peker på at det er bekymringsverdig at det mangler kunnskap om avhengigheten til satellittbaserte tjenester, gitt den økende trusselen mot disse tjenestene både på bakken og i verdensrommet [1]. Dette gjelder særlig PNT med begrensede alternativer til GNSS.

Økt bruk av PNT, særlig GNSS, har skapt stor verdi i form av sikkerhet, økonomi og effektivitet i flere samfunnssektorer i Norge. Navigasjon er en hverdagsfunksjon for mange, og flere sektorer har tatt i bruk nøyaktig tid og posisjon fra satellitter for å operere trygt og effektivt. GNSS tilbyr svært nøyaktig tid, synkronisert mot en felles referansetid. Behovet og bruken av GNSS blir gjerne større ved økt digitalisering og automatisering i form av distribuerte systemer som krever nøyaktig tid og posisjon. Den realiteten har også skapt en omfattende avhengighet til et system med kjente sårbarheter.

GNSS-signalet er svært svakt når det når jordens overflate, og er dermed sårbart for forstyrrelser (interferens) fra romvær eller menneskeskapte signaler. Brukere av GNSS, også militære systemer [2], har erfart flere tilfeller med forstyrrelser mot signalet, og antallet forstyrrelser har økt betydelig siden 2022 [3]. Slike forstyrrelser innebærer både tap av signalet men også forfalskede signaler. I en rapport av *The International Institute of Strategic Studies* viser forfatterne til en økende trend av hybrid krigføring i Europa etter 2022 [4]. Rapporten beskriver blant annet tilfeller av GNSS-forstyrrelser, særlig i Nord-Norge og i Baltikum og Østersjøen. I Norge har det blitt avdekket omfattende forstyrrelser i GNSS-signaler i Øst-Finnmark, noe som har skapt stor bekymring blant myndighetene [5]. Figur 1.1 viser økningen i hendelser av radiofrekvensinterferens (RFI) mot GNSS i Norge de siste årene. I krig og konflikt brukes GNSS-forstyrrelser i form av RFI for å beskytte egne systemer mot GNSS-styrte våpen.

De åpne trusselvurderingene til Etterretningstjenesten i 2025 og 2026 pekte også på trusler mot satellitter. I tillegg til RFI inkluderer dette både kinetiske, ikke-kinetiske og cybertrusler mot både rombasert og bakkebasert infrastruktur [6]. I 2026 understreker Etterretningstjenesten at slike kapabiliteter og trusler fortsatt er under utvikling, samtidig som kommersiell romvirksomhet øker, og peker dermed på verdensrommet som en mulig arena for krigføring [7].



Figur 1.1. Antall dager med GNSS-utfall per år. Fra 2024 har forstyrrelser blitt normaltstanden, ifølge Nkom. Datakilde: Nasjonal kommunikasjonsmyndighet (Nkom).

Norges forsvarsevne er avhengig av at sivile funksjoner som transporttjenester og kraftforsyning fungerer i hele krisespekteret [8], og kritiske samfunnsfunksjoner utgjør grunnlaget for totalforsvarsevnen [9]. Totalberedskapsmeldingen belyser dette med løftet om å «sørge for at det sivile samfunnet er forberedt på krise og krig, og utvikle et samfunn som understøtter militær innsats, og som motstår sammensatte trusler» [8]. Romteknologi og satellitter som GNSS spiller en stor rolle for flere kritiske samfunnsfunksjoner og for å ivareta sikkerhet og beredskap [8]. Siden flere kritiske samfunnsfunksjoner er avhengig av et sårbart signal fra GNSS, kan forsvarsevnen og samfunnets motstandsdyktighet svekkes dersom GNSS-signalet faller bort eller forstyrres, enten tilsiktet eller utilsiktet. Robust PNT er viktig for vår nasjonale og kollektive forsvarsevne. Den årlige internasjonale Jammertesten¹ arrangert på Andøya har avdekket flere sårbarheter hos brukere av GNSS og bidrar til å styrke kunnskapsgrunnlaget.

1.1 Formål og avgrensninger

I 2025 fikk Forsvarets forskningsinstitutt (FFI) i oppdrag av Nærings- og fiskeridepartementet å kartlegge samfunnets avhengigheter av satellittbasert PNT i Norge og de medfølgende sårbarhetene som medfører risiko for totalforsvaret. Vurderingen skal også belyse behov og muligheter for risikoreduserende tiltak. Arbeidet skjer parallelt med flere andre utredninger om problematikken for å bidra til å øke motstandsdyktigheten knyttet til bruk og behov for PNT. Dette inkluderer Menon Economics [10] sin samfunnsøkonomiske analyse og Direktoratet for

¹ Jammertesten på Andøya er et åpent arrangement som tilrettelegger for testing av GNSS-utstyr mot forstyrrelser i et kontrollert miljø.

samfunnssikkerhet og beredskap [11] sin risikoanalyse om manipulering av satellittbaserte tidssignaler. Vår rapport diskuterer også bruk av andre satellittbaserte tjenester i samfunnet og mulige trusler og farer, men de inngår ikke i kartleggingen og vurderingen av kritiske samfunnsfunksjoner.

Samfunnets bruk av satellittbasert PNT er omfattende. Vi har derfor avgrenset studien til å dekke utvalgte kritiske samfunnsfunksjoner og vil for disse vurdere hvilken betydning bortfall av PNT har for totalforsvarsevnen. Vi har også tatt utgangspunkt i å kartlegge og vurdere sårbarheter knyttet til bruk av GNSS på sektor- og undersektornivå, og ikke i tilknytning til virksomhet eller på aktørnivå.

Kartleggingen av bruksområder og behov ble gjort ved å gjennomgå litteratur om bruk av PNT i sektorene og subsektorene og gjennom diskusjon med norske fageksperter hos sektorene under semistrukturerte intervjuer og gruppeintervjuer. En risikobasert tilnærming ble brukt for å vurdere betydning som bortfall av satellittbasert PNT vil ha for totalforsvaret. Metode og avgrensning er beskrevet nærmere i vedlegg A.

1.2 Rapportens struktur

PNT og satellittbaserte tjenester i Norge samt kartlagte bruksområder er presentert i kapittel 3. Deretter beskrives aktuelle og mulige trusler og farer mot satellittsystemer i kapittel 4. I kapittel 5 presenterer vi risikovurderingen for totalforsvaret. Risikoreduserende tiltak er presentert i kapittel 6.

2 Totalforsvar og PNT

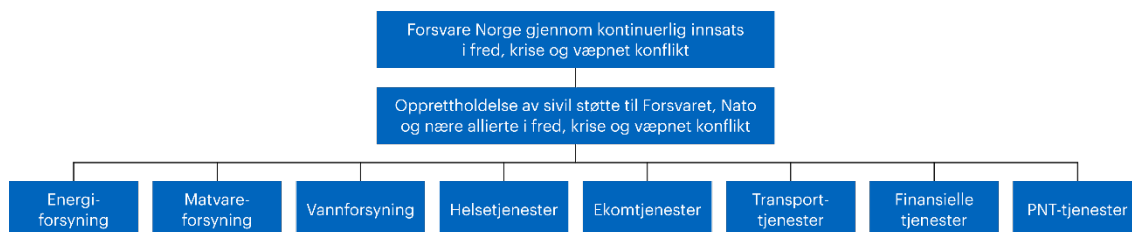
Totalforsvarskonseptet omfatter gjensidig støtte og samarbeid mellom forsvarssektoren og det sivile samfunnet i tilknytning til hendelser i fred, krise og krig. I totalberedskapsmeldingen fra 2025 fremhever regjeringen at totalforsvaret skal bidra til «utnyttelse av landets samlede ressurser innenfor forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering» (s. 29) [12].

Å opprettholde kritiske samfunnsfunksjoner i hele krisespekteret vil ha stor betydning for nasjonal styringsevne, sivil støtte til militære operasjoner og befolkningens trygghet. Sektorer som bidrar til å opprettholde NATOs syv grunnleggende forventninger til sivil motstandsdyktighet er særlig viktige. Disse forventningene er [13]:

- sikkerhet for kontinuitet i nasjonale styringssystemer og kritiske offentlige tjenester
- robust energiforsyning
- evnen til å håndtere ukontrollerte forflytninger av mennesker
- robust mat- og vannforsyning
- evnen til å håndtere masseskader
- robuste kommunikasjonssystemer
- robuste transportsystemer

Evnen til å opprettholde sivil støtte til militære operasjoner er av stor betydning for Norges nasjonale og kollektive forsvarsevne. Med utgangspunkt i NATOs syv grunnleggende forventninger har FFI i en tidligere studie beskrevet hvilke kritiske samfunnsfunksjoner som er særlig viktige for sivil støtte til militære operasjoner, se figur 2.1 [9].

Selv om NATO ikke har uttrykt eksplisitte forventninger til motstandsdyktighet i PNT-systemer (posisjon, navigasjon og tid), er den likevel av stor betydning for totalforsvarsevnen fordi kritiske samfunnsfunksjoner som transportsystemer, kommunikasjonssystemer og energiforsyning er avhengig av PNT. Å forstå sårbarhetene som kan oppstå som følge av de direkte og indirekte avhengighetene som de kritiske samfunnsfunksjonene har til PNT, og særlig til GNSS, er derfor av stor betydning.



Figur 2.1 Totalforsvarsfunksjoner fra FFI-rapport 22/01207 [9].

GNSS er sårbart på grunn av svært svake satellittsignaler som lett kan forstyrres eller forfalskes. Systemets evne til å levere presis PNT er også avhengig av bakkebasert infrastruktur som kan bli utsatt for fysisk sabotasje eller ødeleggelse. Disse sårbarhetene kan føre til uønskede konsekvenser for totalforsvaret gitt samfunnets omfattende avhengighet til nøyaktig, presis og pålitelig PNT – noe som flere grunnleggende samfunnsfunksjoner, særlig transporttjenester, energiforsyning og elektronisk kommunikasjonstjenester, krever.

Upålitelige PNT-tjenester kan gå utover sivilbefolkningens trygghet, for eksempel ved at navigasjonsløsninger blir utilgjengelige eller gir feilaktig informasjon. Bortfall av PNT kan også skape forsinkelser og nedsatt funksjonsevne i kritiske samfunnsfunksjoner som kan medføre fare for liv og helse. Dette er beskrevet i flere nasjonale utredninger [14-17], og risikoen forsterkes særlig under krisesituasjoner, der PNT normalt bidrar til rask og effektiv handling (reparasjonsarbeid, luftambulans, med mer). Risiko og betydning for norsk totalforsvar beskrives nærmere i kapittel 5.

3 PNT og satellittbaserte tjenester i Norge

Betegnelsen PNT (posisjonsbestemmelse, navigasjon, og tidsbestemmelse) brukes for å beskrive hele systemet som muliggjør tilgang til posisjon, navigasjon og tid. Per 2026 er det få alternativer som kan tilby like nøyaktig PNT som GNSS, og slik situasjonen er i dag, har Norge ingen andre systemer som kan tilby samme ytelse. Dette kapitlet beskriver satellittbaserte tjenester i Norge, bruksområder for PNT og hvilken rolle satellittbasert PNT kan ha.

3.1 Romvirksomhet

3.1.1 Globale navigasjonssatellittsystemer – GNSS

GNSS består av satellittkonstellasjoner som går i mellombane (MEO – *medium Earth orbit*) og sender kontinuerlig data til jordoverflaten slik at GNSS-mottakere kan beregne sin egen posisjon og nøyaktig tid. GNSS utnytter tildelte frekvensområder i det såkalte L-båndet av det elektromagnetiske spektret (se Tabell 3.1). I dag finnes det fire globale (verdensdekkende) satellittsystemer for navigasjon: amerikanske GPS, europeiske Galileo, kinesiske BeiDou og russiske GLONASS. I tillegg har vi regionale satellittsystemer (ofte avgrenset til spesifikke land) som den indiske IRNSS og japanske QZSS.

Tabell 3.1 GNSS-frekvensbånd for GPS, Galileo, GLONASS og BeiDou [MHz]

Bånd	GPS	Galileo	GLONASS	BeiDou
L1/E1	1575.42	1575.42	~1602	1561.098 / 1575.42
L2/E6	1227.60	1278.75	~1246	1268.52
L5/E5	1176.45	1176.45	1202.025	1176.45 / 1207.14

Satellittene er utstyrt med atomklokker som er synkronisert med hverandre og bakkestasjoner. En mottaker bruker tidsinformasjon i satellittsignalet til å beregne avstanden opp til satellitten. Når en mottaker på jorden får tak i signaler fra fire eller flere satellitter, kan posisjonen beregnes med god nøyaktighet. Samtidig vil denne prosessen korrigere mottakerens egen klokke til å bli svært presis. Atomklokkene om bord i satellittene er nøkkelen til navigasjonsfunksjonen – feil på et mikrosekund kan føre til flere hundre meter feil i posisjonen [18].

Det bakkebaserte segmentet av GNSS er avgjørende for å synkronisere satellitter, sende korreksjonsdata og overvåke tilstanden til konstellasjonen. Bakkesegmentet består av et nettverk av infrastruktur som mottar og sender signaler til GNSS-satellittene. Hver konstellasjon har et

bakkesegment som består av ett eller flere kontrollsentre, med støtteinfrastruktur spredt geografisk verden rundt.

For å forbedre ytelsen til GNSS finnes både bakkebaserte støttesystemer (GBAS – *ground-based augmentation system*) og satellittbaserte støttesystemer (SBAS – *satellite-based augmentation system*). European Geostationary Navigation Overlay System (EGNOS) er et eksempel på SBAS utviklet av EU og Den europeiske romfartsorganisasjonen (ESA) for å forbedre ytelsen til GPS i Europa. Systemet består av tre geostasjonære satellitter og en rekke bakkestasjoner (inkludert fem plassert i Norge). Norge, gjennom Direktoratet for romvirksomhet, har spilt en stor rolle i å utvide EGNOS sin funksjonalitet til nordområdene.

Kartverkets jordobservatorium på Ny-Ålesund er en del av et globalt nettverk av stasjoner som spiller en viktig rolle i å definere og vedlikeholde den globale geodetiske referanserammen [19, 20]. Blant annet overvåker og måler stasjonen endringer i jordklodens bevegelser. Denne informasjonen, som må oppdateres kontinuerlig, er en viktig forutsetning for at GNSS og andre satellittbaserte tjenester, som jordobservasjon, fungerer. En rapport utgitt av FN i 2024 påpeker svakheter i verdikjeden for den globale geodetiske referanserammen som inkluderer sårbarheter i bakkeinfrastruktur, tap av kompetanse og ressurser, mangel på styringsmekanismer og lite bevissthet om betydningen av geodesi [21].

Multi-konstellasjon- og multi-frekvens-GNSS

I 2026 er stadig flere mottakere egnet til å beregne posisjon og tid med signaler fra flere ulike konstellasjoner samtidig (multi-konstellasjon-GNSS-mottakere). Dette gir tilgang på flere satellitter og betyr i teorien at man kan klare å estimere sin egen posisjon med signaler fra for eksempel én Galileo-satellitt og tre GPS-satellitter. Ved å benytte flere satellittkonstellasjoner kan man også få tilgang til flere frekvensbånd (multi-frekvens-GNSS-mottakere, se Tabell 3.1), noe som gir større motstandsevne mot forstyrrelser i tilfeller hvor kun enkelte av frekvensbåndene er påvirket. Hvorvidt man har evne til å utnytte flere konstellasjoner og frekvenser, kommer an på egenskapene i både mottaker og antenne.

3.1.2 Andre satellittbaserte tjenester

Satellitter i lavbane (LEO – *low earth orbit*) og geostasjonær bane (GEO – *geostationary earth orbit*) er gjerne utstyrt med forskjellige nyttelaster som også er brukt til jordobservasjon og kommunikasjon.

Kommunikasjon var det første bruksområdet for kommersielle romtjenester. Kringkastings-satellitter i geostasjonær bane, slik som Space Norway sine Thor-satellitter, tilbyr TV-tjenester i Norge. Space Norway sitt HEOSAT-prosjekt, eller Arctic Satellite Broadband Mission (ASBM), ble skutt opp i 2024 i høyelliptisk bane (HEO) og skal tilby bredbåndsdekning i Arktis [22], for både militære og sivile brukere [23]. Kommunikasjonssatellitter muliggjør toveissamtaler som blant annet brukes mye i maritim kommunikasjon. Kommunikasjonssatellitter brukes også til nettverksbaserte tjenester til for eksempel overvåking og drift av kontrollsystemer [24].

Lavbanekonstellasjoner av kommunikasjonssatellitter kan tilby både bredbåndsinternett og dataoverføring. Disse har vært i stor utvikling de siste årene, særlig de kjente kjempekonstellasjonene StarLink og OneWeb [25]. Slike konstellasjoner kan i noen grad bli brukt til PNT, noe som diskuteres videre i vedlegg B. GNSS støtter også lavbanekonstellasjoner og forbedrer nøyaktigheten og tilgjengeligheten i dataene, særlig i polare og landlige områder [26].

Enkelte satellitter som FFIs ArcSat-1, skal også bidra til å øke rekkevidden på bakkebasert taktisk radiokommunikasjon hos Forsvaret [27].

Satellitter utstyrt med ulike typer sensorer brukes i dag til å overvåke og forske på jordens overflate og atmosfære. Slike satellitter bidrar blant annet med meteorologiske data og miljø- og klimaovervåking. Copernicus-programmet ble utviklet for dette formålet av EU, av ESA og gjennom det europeiske økonomiske samarbeidsområdet (EØS). Programmet består av syv satellitter utstyrt med blant annet radar og optiske sensorer [28]. Copernicus bidrar til overvåking av for eksempel skipstrafikk, havis, vegetasjon, avlinger, sjøforhold, og naturhendelser. I tillegg gir observasjoner fra satellitter (som satellittene til Eumetsat og amerikanske NOAA – *National Oceanic and Atmospheric Administration*) viktige bidrag til moderne meteorologiske modeller [25].

Norge har utviklet flere satellitter for å øke situasjonsforståelsen i det maritime domenet. NorSat- og AISSat-satellittene er utstyrt med AIS (Automatisk identifikasjonssystemer)²-mottakere for å forbedre dekning av deteksjon av AIS-signaler. Satellittene videreformidler AIS-signaler i områder der landbaserte AIS-mottakere ikke har dekning, til stor nytte for søk- og redningstjenester. NorSat-3 inkluderer også en radardetektor og NorSat-4 er utstyrt med et lavlyskamera. NorSat og AISSat har også betydning for overvåking av ulovlig fiske eller for eksempel for uttømming av grunnvannsreservoarer [25].

3.2 Tidsbestemmelse

Tidsbestemmelse innebærer at man etablerer en nøyaktig og pålitelig referanse for tid basert på en lokal eller ekstern tidskilde. Mange distribuerte systemer krever synkronisert tid for å fungere. GNSS (se boks 3.1) er en globalt tilgjengelig og svært nøyaktig tidsreferanse.

I noen systemer kreves det svært nøyaktig synkronisering – det vil si at nettverksnoder har samme tid ned til nanosekundet, eller en milliarddel av et sekund. For andre systemer kan ett sekund være tilstrekkelig grenseverdi. Noen systemer synkroniserer mot en egen lokal tidskilde, mens mange systemer synkroniseres mot for eksempel en global eller nasjonal referanse.

² AIS samler inn og kringkaster skipssposisjon og er brukt til blant annet antikollisjonssystemer og overvåking av sjøtrafikk.

Boks 3.1: Atomklokker, den internasjonale tidsreferansen og GNSS

En stabil frekvenskilde brukes til å holde takten i et system. Ved å telle antall perioder fra et definert startpunkt kan man måle tid, og slik etableres en klokke. De fleste klokker bruker krystalloscillatorer for å holde takten, men nøyaktig tid (ned til mikrosekundet) bestemmes i dag ved bruk av atomklokker. Atomklokken benytter kvantefysiske egenskaper av visse isotoper, som cesium-133, for å stabilisere frekvensen fra en oscillator. Dette gir en veldig nøyaktig frekvensstandard.

Den første kommersielle kvartsklokken fra 1929 hadde en nøyaktighet inntil ett sekund per 8 måneder, mens dagens atomklokker kan beholde nøyaktighet på ett sekund over flere millioner år [29]. Ett sekund er definert basert på frekvensen av en hyperfinovergang i grunnstilstanden til et cesium-133-atom.

Andre typer atomklokker inkluderer kommersielle rubidiumklokker og hydrogen-maserklokker. GNSS-satellitter i dag er stort sett utstyrt med slike klokker [30, 31]. Rubidiumklokker avviker noen nanosekunder per dag, som betyr at de regelmessig må synkroniseres for å holde nøyaktighet på nanosekundet – noe som er viktig for at GNSS skal fungere. Nyere GNSS-satellitter bruker også hydrogen-maserklokker som masterklokke [32, 33].

Klokkene på GNSS-satellitter synkroniseres opp mot hverandre og utgjør en tidsreferanse for hver konstellasjon, eller GNSST (GNSS-tid), som GPS Time eller GST (Galileo System Time).

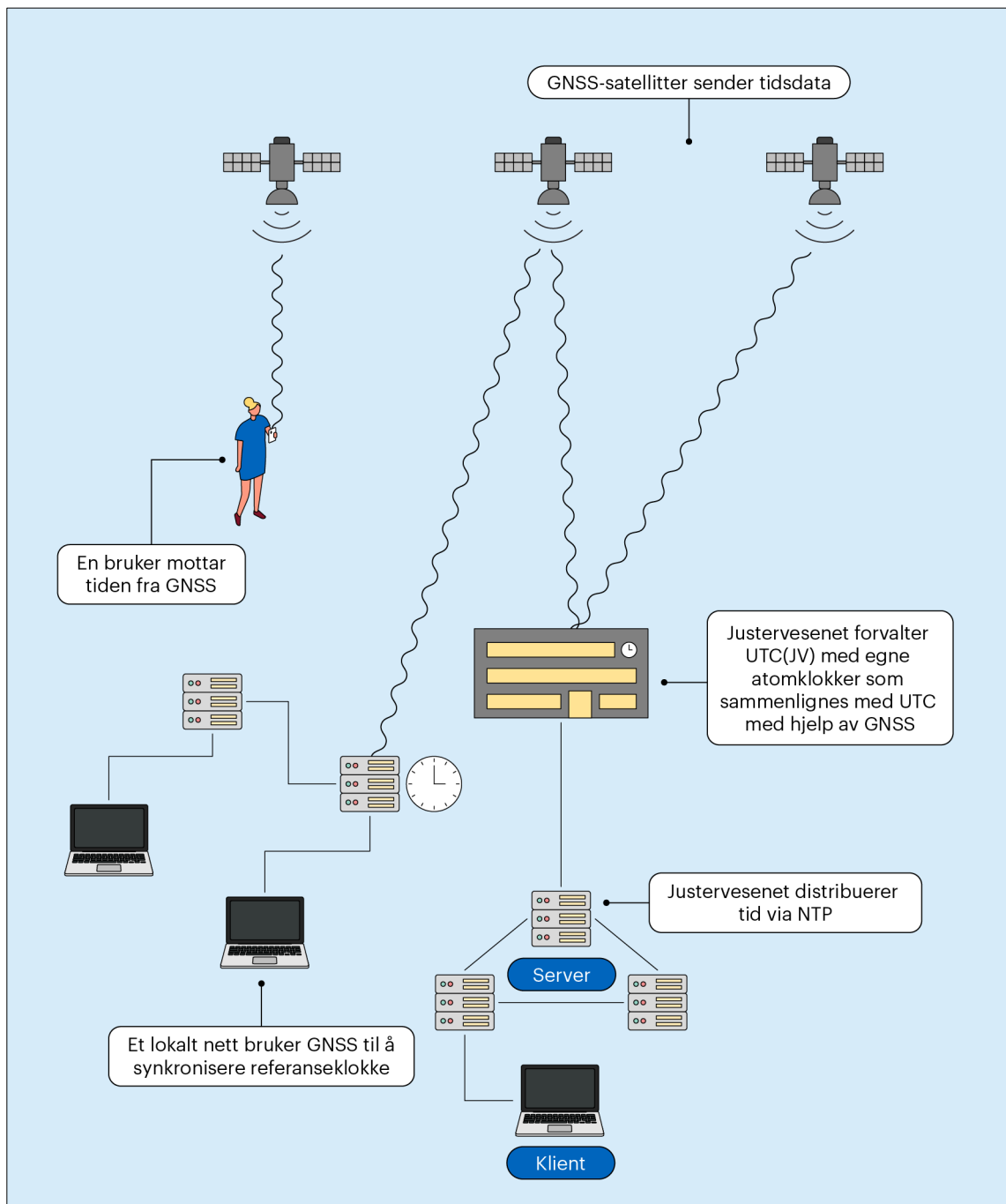
Atomklokker er i dag ryggraden for vår globale tidsreferanse (Coordinated Universal Time – UTC). UTC blir beregnet ved å kombinere frekvensen fra over 450 atomklokker verden rundt, og synkronisert mot tidsreferansen basert på jordens rotasjon (UT1) [34]. Klokkene som inngår i UTC-beregningen, sammenlignes med hverandre ved hjelp av GNSS eller med andre trådløse eller kablede forbindelser.

For større systemer med kritisk behov for synkronisering kan nodene i stedet synkroniseres via kabelbasert tidsdistribusjon, eksempelvis ved bruk av protokoller som NTP (*Network Time Protocol*) og PTP (*Precision Time Protocol*). NTP er brukt for å synkronisere store nettverk med millisekund nøyaktighet, oftest over internett [35], noe som gjør den særlig sårbar for cyberangrep [36, 37]. PTP distribuerer tid med under ett mikrosekund nøyaktighet og krever spesialisert maskinvare [35]. PTP er ofte benyttet til industrielle behov. GNSS kan brukes for å synkronisere klokker i NTP- og PTP-konfigurasjoner, men anbefales ikke som en primærklokkekilde i NSM

sin veileder for sikring av NTP på grunn av sårbarheten for forstyrrelser [38]. GNSS, PTP og NTP til tidssynkronisering er oppsummert i Tabell 3.2.

Tabell 3.2 Oversikt over metoder for tidssynkronisering

Synkroniserings- metode	Nøyaktighet	Virkemåte	Utfordringer
GNSS	< 1 μ s	Hver node i et nettverk får en utgave av UTC-tid direkte fra en GNSS-mottaker.	Sårbar for forstyrrelser i GNSS-signalet. Upraktisk å implementere GNSS-antennene på hver node av store distribuerte systemer [39]
NTP	1 ms	Stratumhierarki på tidskilde og servere. Brukt for synkronisering på internett og andre lukkede nett.	Lav nøyaktighet og direkte sårbar for cyberangrep [36].
PTP	< 1 μ s	«Master-slave»-arkitektur av tidskilder basert på IEEE-1588-standard. Ofte brukt i industri med behov for høy kontinuitet og nøyaktighet.	Behov for spesialisert maskinvare. [35]



Figur 3.1 Forenklet illustrasjon om måter GNSS kan benyttes i systemer for tidsbestemmelse i Norge. Merk at man også kan få og distribuere tid på andre måter (se tabell 3.2). Beskrivelse: Atomklokkene til Justervesenet bidrar til beregning av den globale tidsreferansen UTC som heter UTC(JV) og sammenlignes med UTC ved hjelp av GNSS. Justervesenet tilbyr en NTP-tjeneste synkronisert mot UTC(JV). Lokale nettverk eller andre brukere kan få nøyaktig tid direkte fra GNSS-satellitter.

Justervesenet bidrar til beregningen av den globale tidsreferansen (UTC) med fire atomklokker (to industrielle cesiumklokker og to hydrogen-maserklokker), og sammenligner klokkene sine mot UTC ved hjelp av GNSS [40]. Nasjonale laboratorier i andre land sammenligner klokkene sine også via geostasjonære satellitter eller fiberkabler. Med sine atomklokker forvalter Justervesenet Norges UTC, som heter UTC(JV). De tilbyr en NTP-tjeneste synkronisert opp mot UTC(JV), men det finnes også andre åpne tjenester som NTP-pool som synkroniserer hundre millioner [41] av tidsservere via internett. Figur 3.1 viser eksempler på hvordan GNSS er brukt for å motta eller synkronisere tid.

Selv når internasjonale standarder og veiledere følges, varierer implementering av tidssynkronisering fra system til system. Valg av klokkekilde, utforming av distribusjonsnettverk og antall noder påvirker stabiliteten og nøyaktigheten i systemet. «Holdover» beskriver hvor lenge et system kan opprettholde synkronisering uten eksterne oppdateringer (som fra GNSS). I nettverk med strengt behov for nøyaktig tid brukes gjerne interne atomklokker som redundans til GNSS-tidssynkronisering.

3.2.1 Kartlagte bruksområder for tidsbestemmelse

Tidsbestemmelse er brukt for å synkronisere tidsangivelsen hos ulike brukere og enheter i et nettverk eller system. Synkronisering av tid er nødvendig for kommunikasjonssystemer og tidsstempling av sanntidsdata til for eksempel analyse og hendelseslogging. Dette er viktig for drifts- og kontrollsystemer, tingenes internett (IoT), strømmettet, digitale tjenester og høyfrekvent og automatisert handel. I det følgende beskriver vi hvilke funksjoner tidssynkronisering har i de ulike bruksområdene, uavhengig av synkroniseringsmåte (bakkebasert eller satellittbasert). Disse er oppsummert i slutten av delkapitlet i tabell 3.4.

Elektronisk kommunikasjon

Mobilnett er avhengig av at tid mellom basestasjoner er synkronisert. Spesielt 4G- og 5G-teknologier krever svært nøyaktig tid for å kombinere flere frekvenser (*carrier aggregation*) fra basestasjoner for å oppnå høy tjenestekvalitet (høy databåndbredde). 5G-nettverket krever at basestasjoner er synkronisert med maksimalt avvik på 3 mikrosekunder for å kunne tilby sømløs kommunikasjon [42]. Det er også behov for mobilnett hos andre samfunnsfunksjoner som jernbanen, nødetatene, og IoT-brukere, og 5G blir enda mer integrert i samfunnet [25]. Kringkasting er også avhengig av at basestasjoner er synkronisert. I sjøfarten kringkaster for eksempel AIS informasjon om skip via basestasjoner som krever tidssynkronisering [43, 44].

Digitale tjenester

Lokale og distribuerte nettverk kan kreve at klienter og servere er tidssynkronisert. Nøyaktig tid hos datasentre har tradisjonelt gjerne blitt brukt for å logge hendelser og sikre synkroniserte operasjoner på tvers av datasentre. Nå har behovet økt for å kunne støtte tidssensitive bruksområder [45]. Dette krever ikke særlig høy nøyaktighet og er ofte basert på NTP. I en standard utviklet av den internasjonale telekommunikasjonsunionen (ITU) anbefales det at tidsstemplene på filer fra ulike kilder må være innenfor 1 ms nøyaktighet [46].

Visse autentiserings- og påloggingsløsninger, for eksempel flerfaktoraутentisering, er avhengig av synkronisert tid. I autentiseringsprotokoller, som Kerberos-protokollen brukt i Windows-servere [47], kreves det at brukerens (eller klientens) tid er innenfor et visst tidsrom [37]. I tillegg vil tilgang til visse programvarer og funksjoner kreve at brukerens tid samsvarer med tiden på digitale sertifikater. Om leverandørens server eller brukerens klient får problemer med tidskilden, kan brukeren miste tilgang til data og tjenester.

Drifts- og kontrollsystemer og IoT

Synkronisering er viktig for overvåking og kontroll av store systemer. Kontrollsystemer som SCADA (*Supervisory Control and Data Acquisition*) krever for eksempel nøyaktighet på rundt 100 ms [48] for å tidsstemple hendelser i riktig rekkefølge. SCADA brukes gjerne til å overvåke og kontrollere industrielle prosesser [49]. Synkronisering er viktig i tungindustri, for eksempel i jern- og stålverk, gruvedrift og bedrifter som fremstiller tyngre produksjonsutstyr [50] til både strømfordistribusjon og styring av prosesser [49]. Kontrollsystemer er også viktig i for eksempel kraftsystemet, jernbanen og vann- og avløpssystemer.

IoT er et samlebegrep for et system av noder som produserer og bruker data for å skape et felles operasjonsbilde [51]. Dette brukes til for eksempel integrasjon av flere sensorer for strukturell helseovervåking, trafikkstyring i intelligente trafikksystemer, smarthjem, smartbyer, smarte strømmett [51, 52] og presisjonslandbruk [53]. IoT krever tilstrekkelig tidssynkronisering, noe som kan oppnås ved ulike typer synkroniseringsprotokoller som oftest spores til GPS eller GNSS [51]. Moderne kontrollsystemer krever tilstrekkelig tidsstempling av dataene som fanges opp, og tilstrekkelige kommunikasjonssystemer for overføring av data og kommandoer. Petrov mfl. beskriver konsekvenser av usynkroniserte noder i distribuerte IoT-systemer som inkluderer utløsning av alarmer, feil i beslutningstaking, unødvendige utgifter og fysisk ødeleggelse av utstyr [46].

Økt digitalisering og automatisering øker kravet på nøyaktighet i IoT-systemer. For eksempel har industrielle bruksområder som synkroniserte bevegelser og robotikket behov på under millisekundet [54].

Høyfrekvent og automatisert handel

For institusjoner som tilbyr finansielle tjenester, gjelder MiFID II-regelverket utviklet av EU (EU-direktiv 2014/65/EU). Dette er pålagt i Norge under verdipapirhandelloven [55, 56]. Artikkel 50 i direktivet beskriver krav til synkronisering av klokke for alle finansielle institusjoner. Type rapportert informasjon om hendelser inkluderer tidspunkt av handel og tilsvarende publikasjonstidspunkt, transaksjoner, og hendelser som påvirker transaksjoner. Regelverket spesifiserer nøyaktighet i form av både avvik fra UTC og oppløsning hos deltakere av handelsplasser, oppsummert i Tabell 3.3.

MiFID II-regelverket beskriver at tidsavvik fra UTC for *operatører* av handelsplassene (børsen) skal være maks 1 ms, med minimum 1 ms oppløsning hvis det er en forsinkelse i oversendelse som er mer en 1 ms. Hvis tidsforsinkelsen mellom systemer er mindre enn 1 ms, skal det være maks 100 μ s tidsavvik og minimum 1 μ s oppløsning.

Tabell 3.3 Oversikt over nøyaktighetskrav fra MiFID-regelverket [57].

Type aktivitet	Maks avvik fra UTC	Oppløsning av tidsstempel
Høyfrekvenshandel	100 μ s	$\leq 1 \mu$ s
Telebaserte handelssystemer	1 s	≤ 1 s
Andre prisforespørselssystemer	1 s	≤ 1 s
Slutføring av forhandlede transaksjoner	1 s	≤ 1 s
All annen aktivitet	1 ms	≤ 1 ms

Strømnett

Frekvensen i kraftsystemet ligger normalt rundt 50 Hz og holdes i normal drift innenfor om lag $\pm 0,1$ Hz. Avvik kan føre til en rekke feil som kan ha konsekvenser for sluttbrukeren. Hvis frekvensen er målt over eller under en viss margin, er det et frekvensavvik, og reserver må brukes for å balansere systemet. Det finnes likevel automatisk vern som slår inn for å beskytte komponenter i systemet fra permanent skade. Informasjon fra de ulike synkroniserte nodene er avgjørende for å oppdage avvik og kontrollere frekvensen, men det krever at tiden er synkronisert på mikrosekundnivå.

Tabell 3.4 Oversikt over bruksområder for tidssynkronisering.

Bruksområde	Behov for synkronisering	Eksempler på berørte samfunnsområder
Elektronisk kommunikasjon	Nøyaktig tids- og frekvenssynkronisering blant basestasjoner i mobilnett og andre radionett.	Ekom Jernbane Nødetater Sjøtransport Luftfart
Digitale tjenester	Tilgang til digitale tjenester over internett, som skytjenester, eller lukket nett krever at brukere og datasentre er synkronisert opp mot en felles tidsreferanse. Sertifikater, sikre påloggingsfunksjoner, og dataforespørsler kan kreve samsvarende tid.	Alle kartlagte samfunnsområder
Tidsstemplet data til hendelseslogging og analyse	Til analyse og hendelseslogging bør tidsstemplet data fra forskjellige enheter være synkronisert til en felles tidsreferanse. For eksempel data fanget av satellitter, transaksjonsdata og digital aktivitetslogging. Feil rekkefølge på data kan for eksempel ugyldiggjøre data til analyse og forskning.	Nødetater Finans Kraft
Drift- og kontrollsystemer og IoT	Synkronisering blant sensorer og datanoder i IoT og kontrollsystemer samt kommunikasjonsnett. Krav på nøyaktighet varierer blant industrier og bruksområder. Feil i sensordata og kommunikasjonsfunksjonen kan føre til mekaniske feil, alarmer og data med feil tidsstempling.	Kraft Jernbane Olje- og gass Vann og avløp Landbruk
Strømnett	Synkronisering i utstyr og kommunikasjonsnett til feillokalisering, overvåking og kontroll av strømforsyning	Kraft
Høyfrekvenshandel og automatisert handel	Nøyaktig synkronisering til felles tidsreferanse blant deltakere og operatører av handelsmarkedene.	Finans

3.3 Posisjonsbestemmelse

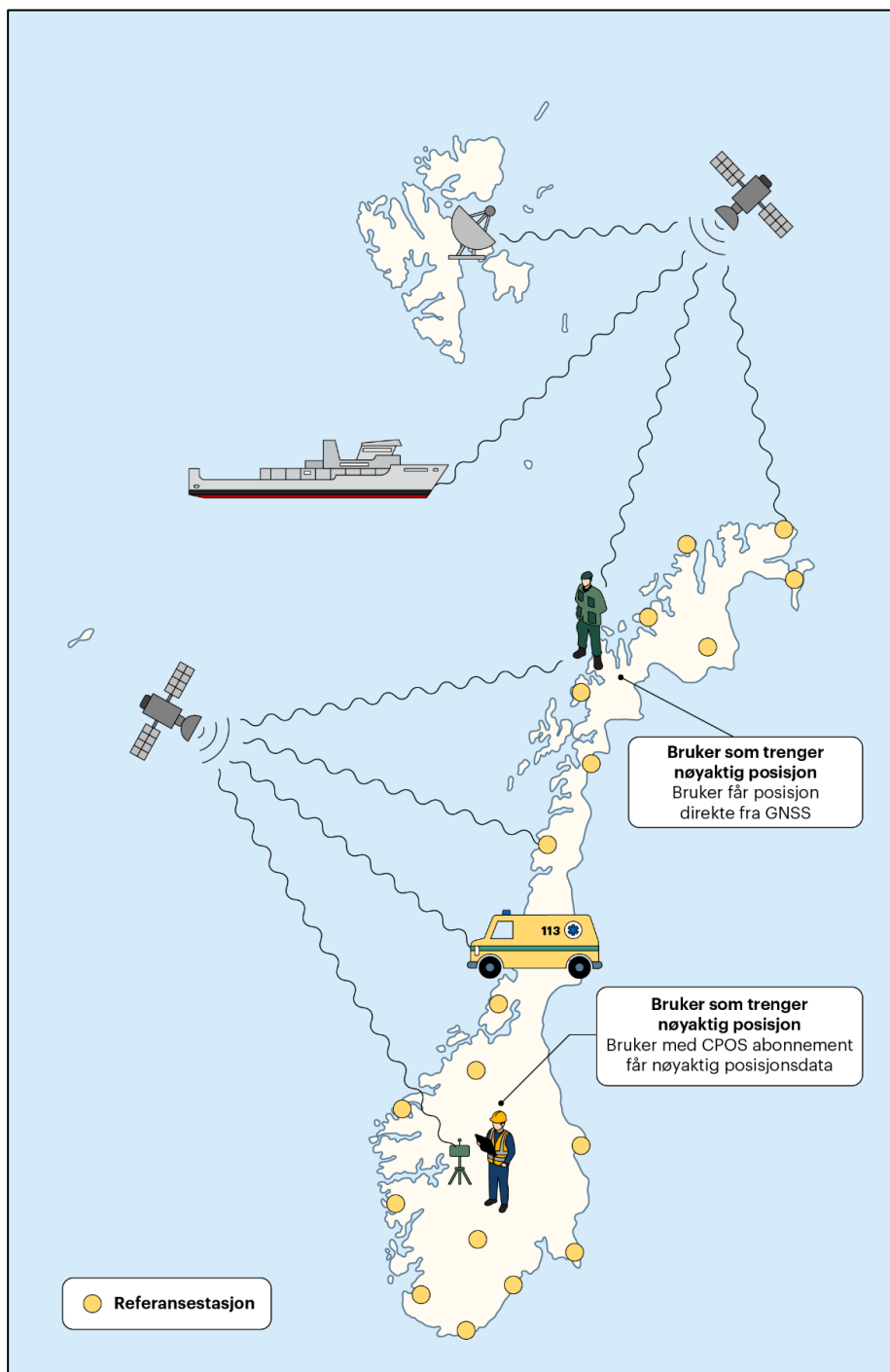
Posisjonsbestemmelse er her definert som bruk av koordinater for å bestemme posisjon i henhold til en kartreferanse. Navigasjon handler om å finne riktig reiserute på vei til målet. En forutsetning for å navigere seg trygt frem er å vite sin egen posisjon, fart og retning, i tillegg til å ha kontroll på når reisen starter, slutter og alle punktene imellom.

GNSS er i dag den vanligste måten å finne sin egen posisjon på, men det finnes også GNSS-uavhengig utstyr til posisjonering og navigasjon, både statisk og dynamisk, for eksempel treghetsnavigasjon, kart og kompass og GNSS-uavhengig landmålerutstyr.

GNSS gir nøyaktige posisjonsestimer omtrent én gang hvert sekund, mens treghetsnavigasjonssensorer, som akselerometer og gyroskop, måler endringer av hastighet og orientering med mye raskere oppdateringsfrekvens enn GNSS. I tillegg er treghetsnavigasjonssensorene ikke sårbare for GNSS-forstyrrelser og kan benyttes for å detektere når GNSS-signalet ikke er til å stole på. Kombinasjonen av GNSS og treghetssensorer er i praksis ofte benyttet fordi disse kan komplementere hverandre.

Den vanligste måten å få posisjon fra GNSS på er å bruke signalet direkte fra satellittene, for eksempel med mobiltelefonen. Det gir en nøyaktighet i posisjonsestimatet på noen få meter, og denne metoden kalles for SPP (*single point positioning*). For å få posisjon med nøyaktighet ned til centimeternivå kan en posisjon korrigeres ved bruk av PPP (*precise point positioning*). Denne metoden innebærer å bruke oppdaterte banedata for satellittene og tofrekvente eller flerfrekvente mottakere for å korrigere for ionosfære- og troposfæreforsinkelser. Enda mer nøyaktig er RTK (*real-time kinematic*) som baserer seg på lokale eller regionale nettverk av referansestasjoner. I Norge leverer Kartverket RTK-tjenesten³ CPOS som gir korreksjonsdata for GPS, GLONASS, Galileo og BeiDou ved hjelp av et nettverk av basestasjoner rundt om i landet [58]. En forenklet illustrasjon for posisjonsbestemmelse i Norge er illustrert i Figur 3.2.

³ Det finnes også andre RTK-leverandører som benytter seg av egne eller Kartverkets referansestasjoner.



Figur 3.2 Forenklet illustrasjon av GNSS til posisjonsbestemmelse i Norge. Posisjonen beregnes basert på signaler fra flere GNSS-satellitter. Stasjonen på Svalbard er Kartverkets jordobservatorium – en del av den bakkebaserte infrastrukturen som sender data til GNSS-satellitter. Referansestasjonene mottar signaler fra GNSS-satellitter for å korrigere posisjonsdata og beregne posisjon ned til centimeter-nivå. Dataene er tilgjengelige fra tjenester som Kartverkets CPOS-tjeneste.

3.3.1 Kartlagte bruksområder for posisjonsbestemmelse

I tillegg til navigasjon gjør posisjonsbestemmelse det mulig å bruke andre viktige funksjoner som landmåling, lokaliseringsteknologi, sanntidsovervåking og innsamling av geodata.

Kartleggingen nedenfor er basert på metoden og avgrensningene beskrevet i vedlegg A. Bruksområdene er oppsummert i tabell 3.5.

Lokaliseringsteknologi

Med lokaliseringsteknologi menes her mobile enheter som sporer og sender posisjonsdata. Det inkluderer flere typer bruksområder som flåtestyring, lokalisering av nødansrop, smittesporing og mobilspill [59].

GNSS brukes til sporing av kjøretøy og andre ressurser i flåtestyringssystemer. Oversikten man får herfra, brukes som underlag for å koordinere oppdrag og operasjoner innen kommersiell transport og i nødetatene. Systemenes ytelse har stor betydning for både kommersiell logistikk og nødetatenes evne til å håndtere nødssituasjoner, og særlig ved store eller samtidige kriser.

Logistikkselskapene bruker i all hovedsak GNSS til posisjonsdata i sine flåtestyringssystemer. Logistikkselskaper er avhengige av data fra et svært distribuert system av transportmidler, mottaksanlegg og kontrollsentre. Innovasjon innen flåtestyring effektiviserer logistikkoperasjoner i stor grad. Bortfall av posisjon og tidsstempling til flåtestyring og navigasjon kan redusere evnen til effektivt å gjennomføre logistikkoperasjoner og levere gods sammenlignet med dagens tilstand.

For å overvåke kystområder hos sjøtrafikkssentralen benytter Kystverket posisjonsdata fra AIS eller LRIT (*Long Range Identification and Tracking*), som får posisjonen fra GNSS. Begge systemene er påbudt gjennom både nasjonale og internasjonale regelverk for visse typer fartøy⁴. Sporing av fartøy er viktig for sjøsikkerheten, overvåking av sjøtrafikken og varsling av farlige situasjoner. SAR (*Search and Rescue*)-helikoptre (helikoptre for søk og redning) er også utstyrt med AIS, og redningssentralen bruker AIS for å lokalisere nødssituasjoner.

Alle fiske- og fangstfartøy må sende posisjon periodisk til Fiskeridirektoratet, ved bruk av VMS (*Vessel Monitoring System*). Forskrift om posisjonsrapporteringsutstyr setter krav på 500 m nøyaktighet i rapportert posisjon [61], og utstyret som brukes, må være godkjent av Fiskeridirektoratet [62]. Posisjonen brukes for å overvåke og kontrollere fiskeaktivitet. VMS sender informasjonen over mobilnett eller via satellittkommunikasjon og bruker posisjonen fra GNSS.

Nødpeilesendere til personlig bruk⁵ og til fartøy⁶ eller fly⁷ er i dag ofte utstyrt med GNSS-mottakere sammen med en innebygd AIS-sender som en del av COSPAS-SARSAT⁸. Med denne

⁴ Beskrevet i kapittel 5 av SOLAS-konvensjonen [60]

⁵ PBL – personal beacon locators

⁶ EPIRB – emergency position indicating radio beacons

⁷ ELT – emergency locator beacon

⁸ COSPAS-SARSAT er det internasjonale samarbeidet for et globalt søk- og redningsprogram basert på et nettverk av satellitter og bakkebaserte stasjoner som fanger opp data fra nødpeilesendere.

funksjonen kringkastes posisjonen til nødpeilesenderen til AIS-mottakere innenfor rekkevidde i forbindelse med nødssituasjoner [63]. Nye generasjoner av nødpeilesendere får bedre posisjonsestimater ved hjelp av GNSS-satellitter som er utstyrt med en SAR-transponder. Dette bidrar til å øke nøyaktigheten i peileteknikken, som også benytter seg av LEO- og GEO-satellitter [63, 64].

Andre lokaliseringsteknologier som nødetatene benytter inkluderer AML (*Advanced Mobile Location*), eCall, voldsalarm og omvendt voldsalarm. Førstnevnte kan bruke posisjon fra GNSS i kombinasjon med andre signaler (som Wi-Fi og særlig mobilnett) for å lokalisere nødansrop fra mobiltelefoner [65]. eCall (nødmeldingssystem for kjøretøy) og voldsalarm bruker posisjon fra GNSS [66, 67]. Omvendt voldsalarm eller straffegjennomføring med elektronisk kontroll, altså fotlenke, benytter enten GNSS-uavhengig radiofrekvensbasert sporingsteknologi eller en kombinasjon med GNSS [68]. GNSS har også blitt benyttet i eldreomsorgen i visse kommuner for å lokalisere personer med demens.

Landmåling og sanntidsovervåking

Landmåling innebærer både innmåling og oppmåling for kartlegging og byggearbeid. GNSS-basert måling brukes i større grad enn før, også sammen med manuelle løsninger som totalstasjon med teodolitt (vinkelmåler) og avstandsmåler [69] eller andre typer sensorer. Totalstasjoner har særlig betydning der GNSS ikke er tilgjengelig eller nøyaktig nok, som til bygg- og anleggsarbeid [69, 70]. Mindre kritiske eller omfattende målinger kan ofte utføres med kun GNSS, mens i andre tilfeller kan GNSS bidra til å forbedre og effektivisere målingsarbeidet.

Til store bygg- og anleggsarbeid brukes GNSS eller totalstasjon, eller en kombinasjon av begge, til å konstruere en referanseramme til arbeidet. Dette er for eksempel beskrevet i Avinor sin spesifikasjon om krav til innmåling og Bane NOR sin dokumentasjon om utbygging av jernbanen [71, 72].

Innmåling er viktig for å kartlegge infrastruktur og anlegg i vann- og avløpssektoren. Ledningsregistreringsforskriften setter krav til kartlegging og dokumentasjon for ledninger og annen infrastruktur i grunnen, sjø og vassdrag [73]. I sektoren er krav til innmåling for anlegg spesifisert i VA-normer for hver kommune, som for eksempel skal foregå med totalstasjon, GPS eller annet utstyr med tilstrekkelig nøyaktighet [74].

GNSS, gjerne i kombinasjon med andre sensorer, brukes i dag til sanntidsovervåking av infrastruktur for å måle forskyvninger eller bevegelser i ustabile fjellmasser i og ved demninger og andre vassdragsanlegg [75]. I NVEs veileder for sikkerhet mot fjellskred foreslås det at GNSS brukes sammen med andre sensorer [76]. Bruk av GNSS til sanntidsovervåking av lagringssystemer for karbon og offshore-anlegg har også blitt kartlagt i litteraturen. Her kan GNSS brukes sammen med andre satellittbaserte sensorer⁹ og seismiske data for å oppdage fortrenkning eller grunnsynking [77]. Dette har også blitt kartlagt for norske oljefelt [78].

⁹ InSAR – *interferometric synthetic aperture radar* – som er også brukt til å kartlegge andre typer deformasjoner i landskap

Geodata

Geografiske data (geodata) er posisjonsdata som er samlet inn til en rekke formål som både karttjenester, forskning og analyse for å forstå og visualisere geografiske fenomener [79]. Karttjenester, eller geografisk informasjonssystemer (GIS) har stor betydning for forvaltning og arealplanlegging og for miljøovervåking [80]. GNSS gjør det mulig å samle inn data over store geografiske områder, der posisjonsstempling skjer i sanntid. Et eksempel er bruk av geodata fra GNSS til hydrologiske undersøkelser og radarmålinger fra fly [81].

Geodata kan også brukes for å videre analysere mønstre eller til logging. Posisjonsdata fra AIS er for eksempel brukt til å utvikle modeller av skipstrafikk og optimalisere ruter eller gi tidlig varsel om farlige situasjoner [82]. Statens vegvesen setter for eksempel krav til bruk av GNSS til veibygging for å dokumentere utført arbeid.

Navigasjonssystemer

I sjøfarten er GNSS innlemmet i navigasjons- og styringssystemene om bord, og det kombineres som oftest med andre sensorer. Posisjonsnøyaktigheten kan økes ved bruk av støttesystemer (augmentasjonssystemer) som den satellittbaserte EGNOS. Norges bakkebaserte augmentasjonssystem for sjøfart (DGPS) blir lagt ned fra 2026, ettersom skip får lignende nøyaktighet ved bruk dagens GNSS og EGNOS [83].

GNSS brukes også i dynamisk posisjonering (DP) av skip og plattformer, som er viktig innen hav- og petroleumsindustrien. DP kan også benytte andre posisjonsreferanse kilder som kortdistanse radio- og laserbaserte systemer eller fra hydroakustiske sensorer.

Luftfarten jobber i henhold til EU-forordningen om ytelsesbasert navigasjon (eller PBN – *Performance-Based Navigation*), der bruk av GNSS er påkrevd og har blitt godkjent for alle faser av flyvning i Norge [84]. Det skrives i Avinor sin PBN-plan at GNSS-uavhengige systemer i fremtiden vil bli brukt hovedsakelig ved bortfall av GNSS.

Landbasert navigasjon på vei er hovedsakelig basert på GNSS. De fleste nye kjøretøy er utstyrt med GNSS-mottakere som brukes i kartnavigasjonsapplikasjoner i underholdnings- og informasjonssystemer (*infotainment systems*). GNSS til navigasjon på vei kan ha en kritisk rolle hos nødetatene, beskrevet nærmere i kapittel 5.2.11.

GNSS brukes også til navigasjon og automatisk styring (auto-styring) av traktorer og landbruksmaskiner i landbruket. Dette inngår i et større system av IoT i landbrukssektoren for presisjonslandbruk. Vi velger å inkludere det som en navigasjonsfunksjon. Intervjuer med landbruksaktører viste at auto-styring var det mest betydelige bruksområdet for GNSS i presisjonslandbruket.

Tabell 3.5 Oversikt over bruksområder for posisjonsbestemmelse.

Funksjon	Bruksområder	Eksempler på berørte samfunnsområder
Landmåling og sanntidsovervåking	Oppmåling og innmåling for kartlegging og byggearbeid Sanntidsovervåking av bevegelser i strukturer	Veitransport Jernbane Vann og avløp
Geodata	Geofysiske undersøkelser	Olje- og gass
	Mobilitetsdata (menneskelige eller biologiske bevegelser)	Sjøtransport Veitransport
Lokaliseringsteknologi	Lokalisering av personer og hendelser	Nødetater
	Flåtestyring og overvåking	Nødetater Luftfart Sjøtransport
Navigasjon	Transporttjenester	Sjøtransport Luftfart Veitransport Nødetatene

4 Trusler og farer mot GNSS

4.1 Radiofrekvensinterferens – RFI

Signalene fra GNSS er så svake at det skal lite til for å overdøve signalene med forstyrrelser, enten de er naturlige eller menneskeskapte, tilsiktede eller utilsiktede. Radiofrekvensinterferens (RFI) omfatter all radiostøy som påvirker GNSS-signaler. De vanligste naturlige forstyrrelsene som rammer GNSS, skjer i atmosfæren. Følgene av dette vil oppleves som en forsinkelse i signalet i mottakeren og føre til feil i avstandsmålingen til satellitten. Omfanget av disse forstyrrelsene påvirkes av lokal tid, årstid, geomagnetisk aktivitet og solsyklus.

GNSS-signalene kan også påvirkes av menneskeskapte forstyrrelser. Disse forstyrrelsene deler vi gjerne inn i to grupper: tilsiktede og utilsiktede forstyrrelser.

Menneskeskapte forstyrrelser som ikke er tilsiktet, dreier seg om radiostøy som sendes ut på grunn av feil på utstyr. Siden frekvensområdet GNSS opererer i, er øremerket til dette formålet, er det ingen andre systemer som har lov til å sende på disse frekvensene.

Signaler kan også bli sendt ut fra jammeutstyr som forstyrrer GNSS-signalet. De tre typene av tilsiktede forstyrrelser kaller vi jamming, spoofing og meaconing. Disse er oppsummert i tabell 4.1.

De siste årene, særlig siden 2018, har det blitt observert jamming og spoofing i større grad, spesielt i tilknytning til konfliktområder der forstyrrelsene brukes til militære formål [85]. Her kan jammingen for eksempel bli brukt til å beskytte mot angrep fra GNSS-styrte våpen og utstyr. Jamming og spoofing forekommer da ofte i land involvert i konflikt eller krig og forstyrrelser kan også oppstå i regioner som grenser disse landene. Dette kan man tydelig se i kartløsninger som viser ADS-B-rapporteringer¹⁰ fra fly som opplever jamming, spoofing og meaconing, se Figur 4.1.

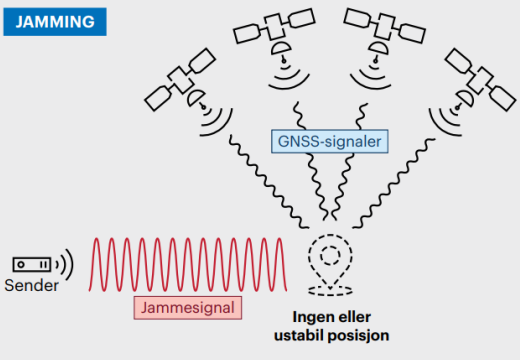
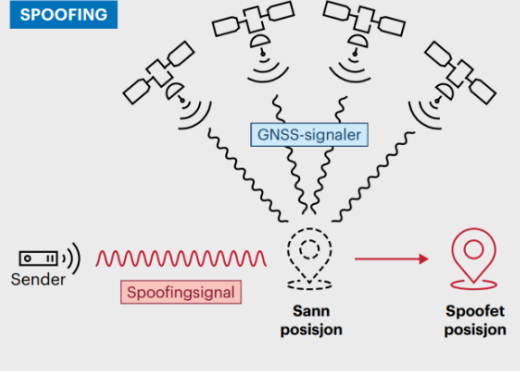
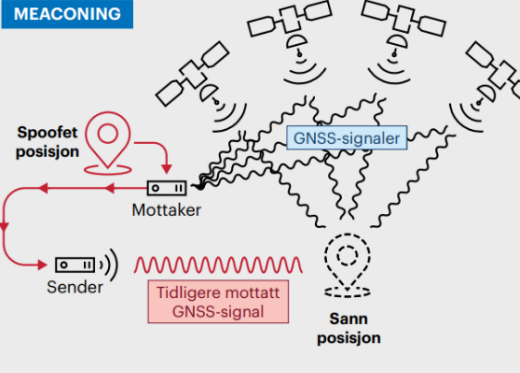
Jamming gjøres også av enkeltpersoner for å skjule posisjonen sin og unngå overvåking og sporing av posisjonen [86], enten om det er fra arbeidsgiveren eller av personvernshenninger [87]. Slike forstyrrelser går utover andre GNSS-brukere. En studie fra 2022 viste at slik ulovlig jamming fra biltrafikken skjedde daglig i de studerte i områdene rundt to flyplasser [88]. En kjent hendelse i Norge illustrerer den faren, da en lastebil som brukte en ulovlig jammer, hindret innflyvningen av luftambulansen [89]. Erfaringer fra testing av GNSS-utstyr mot jamming på den årlige Jammertesten på Andøya (se boks 4.1) viser også at svikt i Wi-Fi-systemer kan skape støy som påvirker GNSS-mottakere [90].

Spoofing av GNSS-signaler er å sende ut syntetiske eller falske satellittnavigasjonssignaler. Dette gjøres gjerne med en GNSS-simulator hvor man kan manipulere både tid og sted for mottakerne som er innen dekningsområdet til systemet. Sammenlignet med jamming er spoofingsignaler ofte

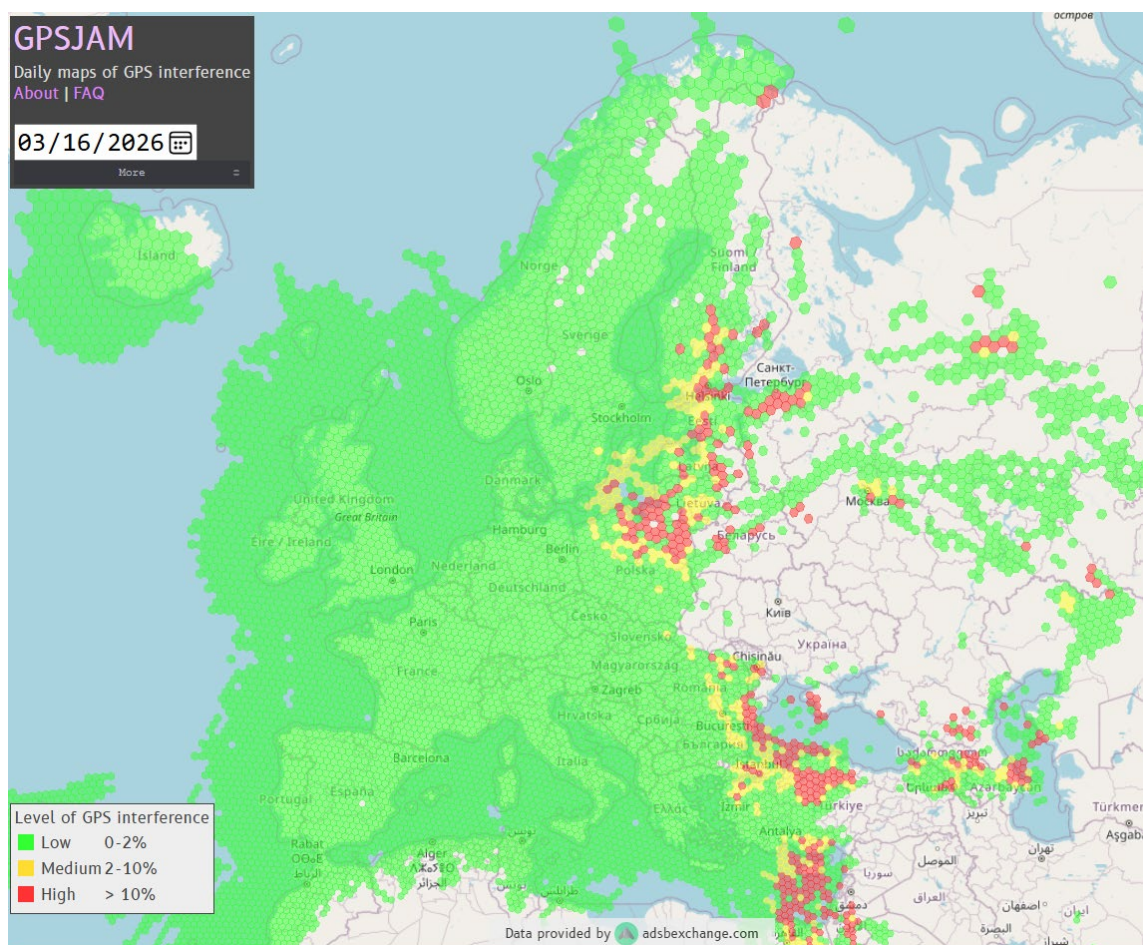
¹⁰ ADS-B (*Automatic Dependent Surveillance-Broadcast*) er et system som sender og mottaker posisjonsdata for fly.

mye svakere. De kan være vanskelig å oppdage dersom en mottaker har en deteksjonsalgoritme som avhenger av mottatt signalstyrke. Spoofingsignalet kan derfor snike seg under terskelverdien for algoritmen. Dette kan gjøre spoofing til en verre trussel enn jamming for mange brukere. Forfalskede tidssignaler kan lage utfordringer for systemer og nettverk som synkroniseres ved hjelp av GNSS-disiplinerte klokke. Manipulasjon av posisjon kan føre til farlige situasjoner i trafikken. Noen GNSS-mottakere har innebygde deteksjonsalgoritmer for spoofing, men de fleste har liten eller ingen beskyttelse mot denne typen angrep.

Tabell 4.1 Oversikt om jamming, spoofing og meaconing.

JAMMING 	Jamming er støy. Støysignaler med de samme frekvensene GNSS benytter, blir sendt ut. Dermed blir mottakerne i nærheten overdøvet. En GNSS-mottaker vil oppleve stor unøyaktighet i posisjonsestimatet eller miste det helt.
SPOOFING 	Spoofing er mer avansert enn jamming. Målet er å få en bruker til å tro at de er på et annet sted enn de er, eller å gi dem feil tidsangivelse. Et falskt satellittsignal blir sendt ut for å lure GNSS-mottakeren. Dette kan for eksempel brukes for å lede fiendtlige droner og missiler ut av kurs. Sammenlignet med jamming er signalstyrken ofte lavere og kan være vanskelig å oppdage.
MEACONING 	Ekte GNSS-signaler blir tatt imot ett sted og sendt ut et annet sted. Påvirkede mottakere vil tro at de er på samme sted som den opprinnelige mottakeren som først tok imot signalene. Til forskjell fra spoofing videreføres her all informasjon som satellittene sender – også krypterte signaler. Sammenlignet med jamming er signalstyrken ofte lavere og kan være vanskelig å oppdage.

Å gjøre meaconing er å motta GNSS-signaler ett sted og sende dem ut igjen et annet. Man kan gjøre det direkte eller via opptak og avspilling. Om man blir utsatt for meaconing vil man i mange tilfeller oppleve lignende effekter som av spoofing. Man vil lese ut feil posisjon og oppleve et tidsavvik tilsvarende tidsforsinkelsen gjennom meaconingsystemet. Tidsavviket vil være lite dersom meaconingsignalet sendes i sanntid sammenlignet med et avspilt opptak. Til forskjell fra spoofing vil også krypterte GNSS-signaler sendes ut av et meaconingsystem, da det i praksis videregirer all informasjon som satellittene sender. Dette kan være utfordrende for brukere som benytter seg av disse signalene.



Figur 4.1 Sivile fly rapporterer integritetsverdier for GPS (Global Positioning System) - nøyaktighet via ADS-B (Automatic Dependent Surveillance–Broadcast)-meldinger, her illustrert på nettsiden gpsjam.org [91]. Rødt og gult indikerer forstyrrelser.

Enkle varianter av jammeutstyr er forholdsvis lett å få tak i på nett, til tross for at det er ulovlig. Det er også relativt enkelt å bygge en spoofer selv [92] ved hjelp av en programvaredefinert radio (SDR) [93] [94] og åpent tilgjengelig kildekode på nett [94, 95].

Boks 4.1 Jammertest på Andøya

Hvert år arrangerer en sammenslutning av norske myndigheter en testarena, Jammertest, der deltakere fra blant annet industri, forskningsmiljøer, og andre myndigheter kan teste GNSS-utstyr mot jamming, spoofing og meaconing. Testen skjer på Andøya i Nordland der kraftig interferens skapes i et kontrollert miljø med minimal påvirkning på samfunnet rundt. Jammertest på Andøya er verdens største, åpne test av sitt slag og har deltakere fra hele verden. Testen bidrar til å avdekke sårbarheter i GNSS-teknologier og bygge motsandsdyktighet i GNSS [97].



Figur 4.2 Jammeutstyr (antennerigg) brukt på Jammertest 2025 på Andøya. Foto: FFI

En annen trussel mot GNSS, i likhet med andre satellittsystemer, er fiendtlige kapabiliteter innen elektromagnetisk krigføring (EK) som kan påvirke kommunikasjon mellom satellitter og bakkestasjoner og mellom ulike bakkestasjoner [96]. Lignende effekt kan også skje på grunn av romvær som utfordrer signalet mellom segmenter.

4.1.1 RFI mot geostasjonære satellitter og lavbanesatellitter

GNSS-konstellasjonene hører hjemme i mellombaneområdet (MEO), mens det befinner seg klart flest satellitter i lav jordbane (LEO). LEO er betegnelsen som brukes for satellittbaner på under 2 000 km høyde. Her er satellittene nærmere nok til å bli utsatt for jamming fra bakken. Mange satellitter benytter GNSS for å estimere sin egen posisjon, og de er derfor utsatt for jamming på disse frekvensene, akkurat som på bakken. Vi har sett at de kraftigste jammerne slår ut mottakerne på satellitter på rundt 500–600 km høyde. Dette er på tross av at jammeantennene gjerne peker horisontalt, det vil si har hovedloben pekende parallelt med bakken og ikke oppover mot satellittene.

I geostasjonære (GEO) og -synkrone baner (GSO), som er på omtrent 35 786 km høyde over ekvator, er satellittene såpass langt unna bakken at de ikke blir påvirket fra GNSS-jammere i nevneverdig grad. Men de er ikke immune mot RFI [98]. I juli 2024 ble det i et møte i den internasjonale telekommunikasjonsunionen (ITU) tatt opp at satellitt-TV-signaler ble utsatt for høyeffektsinterferens som påvirket kringkastingen i Sverige, Luxembourg, Frankrike, Nederland og Ukraina. TV-sendinger ble ikke bare avbrutt, men også erstattet med annet innhold. Ved hjelp av andre satellitt-tjenester ble angrepene lokalisert til å komme fra bakkestasjoner i Moskva, Kaliningrad og Pavlovka i Russland [99].

I prinsippet er all trådløs kommunikasjon sårbar mot RFI. GNSS-signalet er ekstra sårbart på grunn av den lave effekten ved bakkenivå. Dersom samme signal ble sendt fra satellitter nærmere bakken, for eksempel fra LEO, ville det krevd høyere jammeeffekt for å slå ut GNSS-mottakerne.

4.1.2 RFI fra satellitter

Bruken av rommet er i rivende utvikling både sivilt og ikke minst militært. Rommet både er, blir og vil bli forsøkt utnyttet på lik linje som luft, sjø og land for militære formål. Jammeteknologien i en satellitt vil være så å si den samme som på bakken og i lufta. Den store forskjellen ligger i kostnaden med å bringe kapasiteten opp på rett plass i rommet sammenlignet med å montere utstyret på en plattform her nede på jorda. Samtidig er en jammer på jorda enklere å angripe enn en jammer på en satellitt. En GNSS-jammer fra rommet ville kunne dekke et enormt område på bakken og dermed påvirke på begge sider av konfliktlinjen i tillegg til alle sivile brukere med siktlinje til satellitten. En kost-nyttevurdering vil ligge til grunn for om det er formålstjenlig med en jammesatellitt sammenlignet med andre kapasiteter.

Ved å ta høyde for RFI både fra bakken og fra satellitter, gjerne med redundante løsninger som kompenserer for GNSS-bortfall eller ved anti-jammeantennene, kan man potensielt oppnå lengre oppetid for egne satellitter. Men små satellitter har begrenset med plass og strømforsyning til

komponenter som dette, og kompromisser må gjøres etter vurderinger om hvilket utstyr som skal prioriteres på plattformen.

4.1.3 Sårbarhet i beskyttelsestiltak mot RFI

Det finnes i dag flere løsninger med ulike tilnærminger til motvirkning av RFI. Dette inkluderer systemer som detekterer og demper jamme- og spoofingsignaler eller benytter krypterte signaler og autentifikasjonssystemer, som Galileos OSNMA (*Open Service Navigation Message Authentication*).

Forskjellige typer GNSS-mottakere kan påvirkes i ulik grad av RFI. En oppsummering er gjort i Burbank [94], som blant annet viser til forskning på scenarioer som skaper ulik effekt i forskjellige mottakere. Der ble det vist at en mottaker med innebygget motstandsdyktighet mot jamming hadde klare svakheter, og det var et spenn i motstandsdyktighet mot jamming på om lag 15 dB mellom mottakerne i testen. Artikkelen kategoriserer mottiltak mot jamming og spoofing som signalbehandlingsbaserte eller antennebaserte.

Mottakere som kan benytte seg av flere av de fire GNSS-konstellasjonene og også flere av frekvensbåndene (se Tabell 3.1) skal i prinsippet være motstandsdyktige mot jamming av bare én av disse frekvensene. Allikevel viser erfaringer fra de årlige jammertestene på Andøya at også multi-GNSS-mottakere er sårbare mot jamming på kun ett bånd [100]. Resultatene til Kystverket viste også at selv forskjellige mottakere som har samme nivå og sertifisering, vil reagere ulikt på interferens. I tillegg viste testene i 2022 at GNSS-mottakere, også i toppmoderne utstyr, opplevde konsekvenser lenge etter at spoofingen og jammingen stoppet. Dette indikerer en grad av tilfeldighet rundt hvordan man kan forvente at utstyret reagerer på RFI [90].

Ved FFI forskes det på GNSS-anti-jammeantennener og deres ytelse. Disse avanserte antennene gjør en stor forskjell, spesielt mot kraftige jammesignaler. Mange deltakere på Jammertest på Andøya har slike antenner i porteføljen, og det er mye forsknings- og utviklingsaktivitet rundt denne teknologien. En slik antenne kan gjerne erstatte GNSS-antennen koblet til eksisterende mottakere og er sann sett enkel å implementere for utsatte brukere.

4.2 Cyberangrep

Satellittsystemer er avhengig av fungerende IKT-systemer. Dette innebærer både datanettverk og sendere/mottakere for å kommunisere med satellittene fra bakkesegmentet [22]. Menneskelige feil, systemfeil eller tilsiktede cyberangrep kan føre til problemer hos bakkesegmentet som påvirker funksjonen hos GNSS. Bakkesegmentet er den delen av GNSS som er mest utsatt for et cyberangrep, og særlig de fjerntliggende stasjonene [22]. En omfattende undersøkelse av cybersikkerhetsaspektet hos romvirksomheter er beskrevet i FFI-rapporten av Monsen [22], og analysen illustrerer hvordan offensive cyberangrep kan ødelegge eller endre data, tilgang og prosesser utført av romsegmentet. Analysen viser også at slike hendelser er plausible, gitt sårbare verdikjeder og åpenhet i romdomenet.

Cyberangrep mot satellitt-tjenester er en del av krigføringen i Ukraina. I 2022 utførte Russland et cyberangrep mot styringssegmentet til ViaSat sitt KA-SAT-nettverk [101, 102]. Angrepet fikk konsekvenser for både ukrainske brukere av ViaSat sine bredbåndstjenester og omtrent 50 000 brukere i flere land i Europa. SCADA-systemet til vindkraftanlegg i Tyskland, som er styrt gjennom KA-SAT-nettverket, ble også påvirket av angrepet [101].

Mottakere kan også være utsatt for cyberangrep. I en kartlegging utført av universitetet ETH Zurich dokumenterte de 124 tilfeller av cyberangrep mot romsektoren siden fullskalainvasjon av Ukraina i 2022, hvor 2 var rettet mot GNSS. Disse inkluderte angrep rettet mot GNSS-mottakere ved Kreml og russiske vannverk [103]. Kartleggingen inkluderer ikke tilfeller av spoofing og jamming og spesifiserer verken virkemiddel eller konsekvens av disse angrepene.

NASA har også opplevd angrep mot sine bakkestasjoner fra det de mener er knyttet til kinesiske aktører. I 2007 mistet NASA kontroll over to av sine satellitter. I 2014 opplevde National Oceanic and Atmospheric Administration (NOAA) et angrep mot kontrollsegmentet som førte til at systemet ble frakoblet[22]. Om data fra kontrollsegmentet blir kompromittert, kan satellitter få manipulert data som kan føre til at de går ut av bane eller blir koblet fra.

En annen type trussel er skadelig programvare som sprer seg hos romsegmentet – noe som internettkonstellasjoner er særlig utsatt for [22]. Monsen viser til et eksperiment av Thummala [104] som demonstrerte hvordan et slikt angrep kan oppnås. I 2016 førte en teknisk feil, beskrevet som en «*software 'bug'*» [105] under avviklingen av en GPS-satellitt til at flere GPS-satellitter sendte ut feil UTC-korrigeringsinformasjon, noe som igjen førte til et avvik i GPS-synkroniserte klokker.

Forfalskning av signaler, altså spoofing, fra satellittbaserte støttesystemer (SBAS) kan også føre til at mottakere får feil korreksjonsdata. Dette ble testet og oppdaget av Kystverket på Jammertesten og er beskrevet i Kystverkets rapport Status 2025 [106]. Her reagerte ulike mottakere forskjellig på falske beskjeder fra SBAS om integriteten i signalene. Den ene mottakeren som de testet, lot seg lure av spoofet SBAS-signal og forkastet alle de sanne GPS L1-signalene [106].

4.3 Ødeleggelse av fysisk infrastruktur

GNSS er avhengig av både rombasert og bakkebasert fysisk infrastruktur som kan være utsatt for tilsiktede angrep eller naturlige hendelser som ekstremvær, romvær eller kollisjon med naturlige objekter i rommet¹¹. Romsøppel utgjør også en trussel mot fysisk infrastruktur i verdensrommet, særlig for satellitter i lavbane [107].

Det utvikles også rombaserte kapabiliteter, som anti-satellittvåpen, manøvrerbare satellitter og bakkebaserte laservåpen. USA, India, Russland og Kina har utviklet og testet anti-satellittkapabiliteter. Kina har de nevnte kapabilitetene og kan bruke dem til å rette angrep i alle

¹¹ I dag finnes det rundt 2000 kjente asteroider og kometer som er klassifisert som «*potentially hazardous objects*» [[107]]

baner eller forstyrre kommunikasjonen mellom satellitter og bakkestasjoner [96]. Den russiske utviklingen av anti-satellitt-atomvåpen har også fått stor oppmerksomhet [96]. I 2021 gjennomførte Russland en test av et anti-satellittvåpen som slo ut en russisk satellitt. Dette ble deretter beskrevet som en kapabilitet som kan nekte tilgang til og bruk av verdensrommet av USA og USAs allierte [108]. Slike trusler kan ødelegge et stort antall satellitter, som beskrevet av etterretningstjenestens åpne trusselvurdering [7].

Anti-satellittkapabiliteter kan deaktivere enkelte satellitter enten midlertidig eller permanent [107]. Manøvrerbare satellitter kan brukes for å vedlikeholde andre satellitter, men kan også bli brukt til å ødelegge andre satellitter eller dra de ut av bane slik at satellittene blir ubrukelige [25, 109]. I en rapport av CSIS ble det kartlagt ulike typer operasjoner utført av manøvrerbare satellitter i 2024 og 2025 som illustrerer denne kapabiliteten i lavbane og geostasjonær bane [110].

4.4 Bortfall av GNSS i hele krisespekteret

I dette kapitlet beskriver vi hvordan trusler og farer er brukt eller oppstår i ulike deler av krisespekteret. Hensikten er å belyse tenkelige scenarioer for forstyrrelser og bortfall av GNSS.

4.4.1 Lokale forstyrrelser av GNSS

Gråsonekonflikter

Privatpersoner som av ulike grunner ønsker å skjule posisjonen sin, for eksempel på grunn av ulovlig aktivitet eller av personvern hensyn, vil kunne jamme med rekkevidde fra noen få kilometer opptil noen titalls kilometer [87]. Det argumenteres i forskningen til Westbrook for at organiserte kriminelle, terrorister og fremmedstatlige proxy-aktører vil kunne ha kapasitet til å jamme med opp mot 50 kilometer, mens statlige aktører vil kunne oppnå jammeeffekt på flere hundre kilometer [87]. I praksis vil jammeeffekten være begrenset av tilgangen til fri sikt mellom jammer og GNSS-mottaker, og bakkebaserte jammere vil derfor fort begrenses av terrenget rundt. Bos mfl. peker også på faren for systematisk jamming, der en offensiv aktør jammer på en intelligent og målrettet måte for å skape stor effekt [111].

I en gråsonekonflikt bruker aktører ulike virkemidler for å oppnå strategiske mål under terskelen for væpnet konflikt. Dette kan ta form av fysisk ødeleggelse, psykologisk påvirkning og tvang [112]. Forskere har vurdert at målrettede RFI-angrep mot GNSS-brukere kan bli brukt taktisk for å oppnå strategiske og politiske mål [113, 114]. Dette kan innebære for eksempel å spoofe posisjonen til et skip for å lede det inn i en farlig situasjon som grunt vann eller annet territorielt farvann. I en analyse gjort av Lloyds List mistenkes det at posisjonen til det britiske tankskipet *Stena Impero* ble spoofet før det ble arrestert av iranske myndigheter [115]. Selv om det aldri ble bekreftet om dette var på grunn av spoofing, understrekes det at hendelsen hadde politisk betydning [113].

I 2021 ble det rapportert flere tilfeller av krigsskip med forfalsket posisjonsdata (et tilfelle av cyberangrep og ikke spoofing) [116], noe som kan bidra til å skape usikkerhet eller eskalere en geopolitisk konflikt. Et eksempel er at posisjonen til to norske krigsskip trolig ble forfalsket slik

at det fremsto som om de var i russisk territorielt farvann, selv om de ikke var det [117]. Hendelser ble også rapportert av den svenske Försvarsmakten. Slik manipulasjon kan bidra til å skape et fiendebilde og bidra til narrativ om vestlig aggresjon, ifølge forskere i Norge [113, 117].

Krig

Russiske forstyrrelser av GNSS nær Øst-Finnmark er i grove trekk en konsekvens av den pågående krigen i Ukraina og Russlands anspente forhold til NATO. De er beskrevet som et defensivt tiltak av etterretningstjenesten [7] og har ført til at norske fly og skip har mistet navigasjonssignaler [118]. Luft og sjøtrafikken over og i Østersjøen har også vært utsatt for GNSS-forstyrrelser, hvor myndighetene i de baltiske landene har vurdert forstyrrelsene som målrettede hybride hendelser [117, 119], mens andre vurderer at dette også mest sannsynlig er beskyttelsestiltak [120, 121].

Tilsiktet RFI i krig, også kjent som elektromagnetisk krigføring (EK), er et kjent virkemiddel i for å eksempelvis forstyrre motstanderens evne til å bruke GNSS-styrte våpen og droner og for å beskytte eget utstyr. I Ukraina rapporteres det om at jamming av GNSS og satellittkommunikasjon har redusert nøyaktigheten til flere våpensystemer siden fullskalainvasjonen i 2022 – noe som har ført til at våpen har truffet langt fra målet [121, 122]. Jamming av GNSS har vært så omfattende i deler av Ukraina at det også har fått konsekvenser for andre satellittsignaler, for eksempel kommunikasjonssatellitter i lavbane [123].

4.4.2 Omfattende bortfall av GNSS

Tilsiktede handlinger kan også slå ut enkeltsatellitter, konstellasjoner eller signaler for å oppnå en ønsket effekt der motivasjonen kan være å redusere en motstanders tilgang til satellitt-tjenester. Forskerne Bowers og Hiim [96] beskriver et tenkt scenario der Kina bruker ikke-kinetiske virkemidler (som cyber eller andre elektromagnetiske virkemidler) for å forstyrre amerikansk ISR under en konflikt i Stillehavet, noe som de beskriver kan få konsekvenser for NATO-land og føre til kaskadeeffekter for andre satellittsystemer. Andre årsaker til omfattende bortfall, beskrevet i forrige delkapitler, inkluderer både rombaserte og bakkebaserte angrep (cyber eller fysisk).

Kraftige romværshendelser eller et angrep på en GNSS-konstellasjon, enten det er mot rominfrastruktur eller bakkesegmentet, kan føre til omfattende bortfall. En slik situasjon kan føre til at hele Norge og store deler av verden mister tilgang til en eller flere GNSS-signaler. Ved en omfattende nok solstorm, noe som er ventet å skje i snitt hvert 100. år [124], vil andre systemer som strømforsyning, satellittkommunikasjon og annen elektronikk påvirkes direkte. I verste fall vil en slik hendelse anses å kunne få konsekvenser for Norge i et par dager [125]. Vi viser til DSB sin analyse av krisescenarioer fra 2019 for videre beskrivelse av et slikt scenario [124].

5 Hvilken risiko medfører GNSS-forstyrrelser for totalforsvaret?

I det følgende analyserer vi hvilken risiko GNSS-forstyrrelser eller bortfall kan føre til for totalforsvarsevnen. Risiko er analysert for de utvalgte samfunnsfunksjonene¹², og deretter beskriver vi betydningen og konsekvenser for totalforsvaret.

Risiko er definert som potensialet for negative *konsekvenser* som følge av en uønsket hendelse med tilhørende *usikkerhet* [126, 127]. Usikkerheten er både knyttet til sannsynligheten for at hendelsen (GNSS-forstyrrelser eller bortfall) fører til negative konsekvenser og styrken på kunnskapen som risikoanalysen bygger på.

Å vurdere sannsynligheter for at tilsiktede GNSS-forstyrrelser kan inntreffe, er forbundet med høy usikkerhet. Vi har derfor valgt å bruke scenarioer for å håndtere denne usikkerheten, men vi har ikke gjort en vurdering av hvor sannsynlig det er at scenarioene kan inntreffe.¹³ Vi har imidlertid satt som krav at scenarioene må være plausible (det må være mulig eller «tenkelig» at scenarioet kan inntreffe), de må være relevante og de må representere kvalitativt ulike utfordringer. Scenarioene er basert på beskrivelsen av trusler og farer mot GNSS i kapittel 4 og inkluderer følgende:

- **Lokale forstyrrelser av GNSS:** RFI (radiofrekvensinterferens), eller spoofing og jamming, som oppstår i et begrenset område som varer i opptil ett døgn.
- **Omfattende bortfall av GNSS:** bortfall av GNSS-tjenester (tap av GNSS-signal) nasjonalt og i store deler av verden som varer fra dager til en måned.

Utfyllende detaljer om scenarioene er gitt i et gradert vedlegg [128].

Hvorvidt hendelsen får konsekvenser, er knyttet til en vurdering av *sårbarhet* som er særlig knyttet til i hvilken grad samfunnsfunksjonen er avhengig av GNSS. Med dette mener vi i hvilken grad GNSS er brukt til å oppnå PNT-behovet til samfunnsfunksjonen.

Vurderingen av *konsekvenser* er basert på en vurdering av i hvilken grad hendelsen fører til svikt i funksjonsevnen til den kritiske samfunnsfunksjonen. Dette er basert på sårbarhetsvurderingen og betydning PNT har for funksjonsevnen. Her beskriver vi også krav på nøyaktighet særlig knyttet til tidsbestemmelse og konsekvenser avvik kan få. Usikkerhet i vurdering av sårbarhet og konsekvenser er avgrenset til styrken i kunnskapsgrunnlaget vårt.

Kunnskapsgrunnlaget for rapporten bygger på intervjudata, som refereres til i teksten, og litteraturstudier. For å understøtte vurderingen benytter vi også relevant litteratur. Styrken i

¹² Analysen er avgrenset til en vurdering av kritiske samfunnsfunksjoner basert på totalforsvarsfunksjonene beskrevet i delkapittel 2 og vedlegg A.1.

¹³ Her er det viktig å bemerke at feiloppfatninger om sannsynligheten til scenarioene kan føre til feil risikoforståelse.

kunnskapsgrunnlaget er basert på usikkerhet uttrykt av intervjudeltakere og vår egen vurdering av dataene som er tilgjengelig. Usikkerhet er oftest koblet til kompleksitet i samfunnsfunksjonen og skyldes begrensninger i datainnsamlingen eller mangel på data. Merk at risiko er vurdert for funksjonsevnen nasjonalt¹⁴ og sektorvis eller for enkelte aktører og virksomheter nevnt i vurderingen.

Vurderingskriteriene for sårbarheter, konsekvenser, usikkerheter og risiko er gitt i vedlegg A.3. Kriterier for risikovurderingen er også gitt i Tabell 5.1. Risikovurderingen er altså en kvalitativ vurdering av samfunnsfunksjonens sårbarhet og potensialet for negative konsekvenser med tilhørende usikkerhet for hvert scenario. Merk at sårbarhets- og risikovurderingen for de ulike kritiske samfunnsfunksjonene er relativ i forhold til hverandre og tar ikke høyde for andre tilsiktede handlinger som kan medføre risiko for totalforsvaret.

Tabell 5.1 Vurderingskriterier for risiko

Risiko	Kriterium
Høy	Middels eller høy sårbarhet og potensial for store konsekvenser Høy sårbarhet og potensial for moderate konsekvenser Høy usikkerhet
Moderat	Middels sårbarhet og potensial for moderate konsekvenser Høy sårbarhet og potensial for små konsekvenser Lav sårbarhet og potensial for store konsekvenser
Lav	Ikke noe potensial for alvorlige konsekvenser, lav sårbarhet og lav eller moderat usikkerhet

5.1 Vurdering av sårbarheter og konsekvenser

5.1.1 Kraftforsyning

Kraftforsyning er viktig for så å si alle samfunnsfunksjoner, og bortfall kan få store konsekvenser for samfunnets evne til å håndtere kriser og kan føre til tap av liv og helse. Beredskap og sikring av energiforsyningen er derfor «et av de viktigste grepene som kan gjøres for å ivareta samfunnssikkerheten» [129]. Energiloven og gjeldende forskrifter er utarbeidet for å styrke kraftsystemets evne til å kontinuerlig levere strøm til sluttbrukeren [129]. NATO stiller krav til medlemsland om robuste energisystemer. Forstyrrelser i kraftforsyningen kan påvirke militære operasjoner og redusere sivilbefolkningens motstandsdyktighet [130].

¹⁴ Tilleggsinformasjon om betydningen som bortfall av GNSS har for totalforsvarsevnen i Troms og Finnmark, er beskrevet i et gradert vedlegg [128].

Kraftsektoren krever nøyaktig tids- og frekvenssynkronisering til flere funksjoner, både i strømmettet og til kraftproduksjon. For å oppnå Norges klimamål kreves det at kraftnettet utnyttes bedre. Det forutsetter digitalisering som øker behovet for nøyaktig tid. Både datafangst og datakommunikasjon fra utstyr og enheter i kraftsystemet krever nøyaktig synkronisering (se også kapittel 3.2).

I totalberedskapsmeldingen beskrives det at bruk av ny teknologi, skyløsninger, utenlandske leverandører og integrering av ulike systemer som er koblet til internett, øker risikoen for IKT-hendelser i kraftforsyningen [115]. Økt digitalisering er dog en viktig del av elektrifiseringen av samfunnet med tanke på tiltak for å oppnå Norges klimaforpliktelser [124]. «Smart energibruk» som er mer digitalisert og energieffektiv kan bidra til å styrke kraftbalansen og forsynings-sikkerheten [125]. Nøyaktig PNT bidrar stort til å styrke kraftforsyningen og det er viktig at robuste PNT-løsninger er på plass for å redusere mulige sårbarheter.

Sårbarhet

Vi vurderer at kraftforsyningen er middels sårbar overfor forstyrrelser eller bortfall av GNSS. Sårbarheten kan øke til høy hvis det innføres nyere teknologi, slik som sanntidsmålere, særlig om arbeid rundt redundante systemer ikke skjer i parallell.

Kraftsektoren forholder seg til kraftberedskapsforskriften, som setter krav om å styrke evnen til å håndtere uønskede hendelser i systemer. Intervjuobjektene viste til Norges vassdrags- og energidirektorat (NVE) sin veileder [131] til kraftberedskapsforskriften som en kilde som forklarer GNSS-avhengigheten for sektoren og kravet til sikre tidskilder. Forskriften krever sikre klokkekilder hos visse driftskontrollssentre¹⁵ [132]. Bruk av GNSS og systemenes redundans vil variere mellom ulike installasjoner i kraftsektoren. Det er verdt å merke seg at NVE i sin veileder beskriver at den vanligste klokkekilden i kraftforsyningsanlegg og driftskontrollsystemer er GPS med kvartsklokker [131].

I drifts- og kontrollsystemer for kraftsektoren er behovet for nøyaktighet i datasystemer på rundt 10 millisekunder, ifølge NVEs veileder [131]. Tidsstempling for måleverdier og hendelser krever derimot nærmere ett millisekunds nøyaktighet, mens ukonvensjonelle løsninger for sanntidsmåling og automatisering kan kreve nøyaktighet på under ett mikrosekund [131].

NVEs veileder beskriver også flere tiltak som bør iverksettes for å redusere sårbarheten knyttet til GNSS. Dette inkluderer redundans, multi-GNSS-mottakere og egne nøyaktige klokkenoder, for eksempel atomklokker. Statnett har jobbet med å sikre tidsdistribusjon på mikrosekund-nøyaktighet med egne cesiumklokker. Disse er beskrevet i intervjuene og kartleggingen gjort av Justervesenet og Nkom [42].

IoT og kontrollsystemer i kraftbransjen har vært diskutert i rapportene til Farsund mfl. [52] og Røyksund og Valdal [133]. Integrasjon av sensorer i kraftbransjen er blant annet brukt til jordfeilovervåking, overvåking av gass- og oljenivå, tilstandsmåling og data fra vernesystem [133]. Sanntidsmålere som PMUer (*phase measurement unit* eller vektormåler på norsk [134])

¹⁵ Spesifisert i § 7-14 og § 7-15 for driftskontrollssentre av klasse 2 og 3.

blir tatt i bruk i større grad i Norge. Tradisjonelle SCADA-systemer (*Supervisory Control and Data Acquisition* eller overordnet styring, kontroll og datainnsamling) benytter IEC 104-protokollen¹⁶ for kommunikasjon mellom kontrollanlegg og driftssentral, men sektoren beveger seg mot større implementering av IEC61850 og sanntidsmålere, som har strengere synkroniseringskrav [16, 135]. Dette blir enda viktigere for fremtidig elektrifisering. Å redusere sårbarhet knyttet til behov for synkronisering og bruk av GNSS blant PMUer har vært et stort forskningstema [39, 93, 136, 137].

GNSS er også en viktig del av moderne metoder for lokalisering og navigasjon av ressurser (som personell og droner) under vedlikeholds- og reparasjonsarbeid.

Konsekvenser

Vi vurderer at et omfattende bortfall av GNSS vil få moderate konsekvenser for kraftforsyningen, mens kortvarige og lokale forstyrrelser vil få små konsekvenser. Det er større usikkerhet knyttet til vurderingen av konsekvensene som følger av et spoofing-angrep og ved økt digitalisering i fremtiden som dermed øker risikoen.

I intervjudiskusjonene med kraftaktører viste det seg at store avvik i tidssynkronisering kan bety at manuelle systemer må tas i bruk – noe som krever både arbeidskraft og kompetanse og kan redusere effektiviteten i driften. I veilederen til NVE står det at «selv om driftskontrollsystemet hos en KBO-enhet (Kraftforsyningens Beredskapsorganisasjon) ikke er avhengig av nøyaktig tid, så vil bortfall eller feilvisning av tid få driftsmessige konsekvenser» [131]. Bortfall av GNSS vil kreve tilpasningsevne for å ivareta drift over tid, og konsekvensene avhenger av kraftaktørenes robusthet og planlegging. I tillegg tar GNSS-uavhengige løsninger til vedlikeholds- og reparasjonsarbeid lenger tid og krever økt bemanning.

5.1.2 Olje- og gassnæringen og drivstofforsyning

I likhet med kraftforsyning og i tråd med NATOs krav om robuste energisystemer spiller drivstofforsyning en viktig rolle i energisikkerheten i hele krisespektret både for sivile og militære [12]. Drivstoff er viktig for flere samfunnsfunksjoner, særlig for transporttjenester, og har stor betydning for Forsvarets utholdenhet [12, 138].

Forsyning av drivstoff innbefatter hele verdikjeden fra utvinning og ilandføring av olje, raffinering og distribusjon via tankanlegg samt import av drivstoffprodukter [9]. I dette delkapitlet beskriver vi sårbarheter og konsekvenser for hele forsyningskjeden for drivstoff fra utvinning av petroleum (olje- og gassnæringen) til import, produksjon og distribusjon av drivstoffprodukter. Videre i rapporten innebærer «drivstofforsyning» også vurderingen av olje- og gassnæringen.

De fleste drivstoffprodukter er basert på petroleum (råolje og gass). Norge produserer store mengder petroleum og er en av Europas største handelspartnere for råolje [139]. Norge er dermed en viktig aktør for Europas, og NATOs, produksjon og forsyning av drivstoff [140]. Rundt 80 % av raffinerte produkter produsert på Mongstad (Norges eneste raffineri) eksporteres, og Norge

¹⁶ International Electrotechnical Commission

importerer deler av forbruket på diesel, marin gassolje og flydrivstoff [139]. Både råolje og drivstoffprodukter transporteres via rørledninger, skip og tankbiler.

Sårbarhet

Vi vurderer at drivstofforsyning er middels sårbar overfor forstyrrelser eller bortfall av GNSS.

Basert på vår kartlegging og intervjudata er utvinningsfasen i offshore-operasjoner avhengig av flere systemer som krever PNT. GNSS er hovedkilden til posisjon for navigasjonssystemer i både fartøy og helikopter for offshore-operasjoner. Radiofyr er også brukt til navigasjon, men med mindre nøyaktighet, og skipsposisjon er brukt til trafikkovervåking og flåtestyring rundt anlegg, der posisjon også fanges opp av radar. GNSS er også brukt til dynamisk posisjonering (DP) av blant annet borerigger og forsyningsskip. I tillegg er det flere kommunikasjonssystemer (som TETRA UHF og satellittkommunikasjon) til offshore-operasjoner som krever tidssynkronisering.

Offshore-virksomheter legger stor vekt på GNSS-robusthet med tanke på muligheten til å kunne omstille operasjoner for å opprettholde drift uten GNSS. Havindustrien forholder seg til standarden NORSOK[141], som stiller krav til redundans for flere av systemene som er avhengig av PNT. For dynamisk posisjonering er det krav om bruk av flere referansesystemer i tillegg til GNSS-uavhengig utstyr.

IoT har også i økende grad blitt innført i olje- og gassnæringen i forbindelse med produksjon og distribusjon. I 2018 beskriver Gressgård mfl. at integrasjon av sensorer brukes til tilstandsovervåking og prosesskontroll, på en lignende måte som sanntidsmålere i kraftbransjen [142]. Petroleumsnæringen digitaliseres også gjennom bruk av roboter og autonome fartøy, automatisering av boreoperasjoner og digitale oljefelt (digital tvilling) [142], noe som ofte krever store mengder sanntidsdata. I 2021 beskrev Hanssen mfl. at pågående digitalisering i petroleumssektoren utfordret forholdet mellom leverandører, og at det i større grad ble «uklart *hvor* og *hvordan* rene programvarebaserte, dataintensive og nettbaserte tjenester utføres og hvordan ansvar fordeles» [143].

Transport og distribusjon av drivstoffprodukter innebærer både mottak av importerte drivstoffprodukter og distribusjon av drivstoff til sluttbrukere. Behov for GNSS hos transport- og logistiktjenester er diskutert i delkapitler 5.3.6–5.3.10, der vi vurderer at bortfall av GNSS kan føre til redusert funksjonsevne og skape flaskehalser. Dette er på grunn av omfattende bruk av GNSS både til flåtestyring og til navigasjon (særlig for maritim transport av varer).

Konsekvenser

Vi vurderer at kortvarige og lokale GNSS-forstyrrelser vil få små konsekvenser for nasjonal drivstofforsyning, men kan skape forsinkelser i de utsatte områdene. Konsekvenser av omfattende bortfall av GNSS er forbundet med moderat usikkerhet, men trolig vil ikke konsekvensene bli større enn moderate for nasjonal drivstofforsyning.

Under intervjuene kom det frem at offshore-virksomhetene har lang erfaring med forstyrrelser og krevende arbeidsforhold. Det ble nevnt at GNSS har forbedret nøyaktigheten og effektiviteten i operasjoner. Derav kan tap av GNSS føre til tap av denne effektiviteten. Intervjudiskusjoner med

aktøren innen havindustri viser at dynamisk posisjonering kan være sårbart, og man kan risikere stans i operasjoner. Men det er også krav om tre uavhengige referansesystemer, noe som kan redusere konsekvenser ved bortfall av ett av dem.

Derimot kan flere funksjoner være utsatt for umiddelbare konsekvenser som krever at aktiviteter stanses frem til andre løsninger tas i bruk, som også beskrevet i rapporten til Menon Economics [10]. Avhengig av hvilke andre sensorer som er tilgjengelig, kan tap av GNSS bety at operasjoner basert på DP må stanses, og det vil ta noen dager for å gjenopprette operasjoner uten GNSS. Muligheten til å navigere til og fra anlegg uten GNSS vil være avhengig av værforhold og at andre sensorer er tilgjengelig.

Mangel på GNSS til navigasjon vil også føre til forsinkelser i offshore-operasjoner. GNSS øker effektiviteten i offshore-virksomheter, og forstyrrelser i GNSS kan gi effektivitetstap og skape farlige situasjoner, særlig om falske posisjonsdata er brukt.

Tidsavvik i offshore-virksomhetenes kommunikasjonssystemer anses å kun få små konsekvenser for kommunikasjon, ifølge våre intervjudata. Et lengre bortfall vil også gi tid til å tilpasse operasjoner med GNSS-uavhengige løsninger (for både kommunikasjon, navigasjon, og posisjonering).

Økende grad av automatiserte og digitaliserte prosesser inngår i både bearbeiding og distribusjon. I likhet med andre bruksområder som benytter IoT og digitale tjenester vurderer vi at avvik i tidssynkronisering kan føre til driftsproblemer.

GNSS er brukt til flåtestyring og transport av petroleumsprodukter, og bortfall kan øke ledetider for leveranser. Intervjuene dekket ikke transport av petroleumsprodukter utenom offshore-virksomhet, men vurderes ut fra dokumentasjon og diskusjon med havindustrien, transportaktører og logistikkaktører. For eksempel har GNSS-forstyrrelser ført til nedsatt kapasitet i Hormuzstredet, beskrevet i kapittel 5.3.7. Omfattende bortfall globalt kan føre til flaskehalser i flere viktige maritime korridorer og transportruter.

Transport av drivstoffprodukter anses å være noe avhengig av GNSS, men dette vil etter vår vurdering få moderate konsekvenser for nasjonal drivstofforsyning, særlig på grunn av Norges behov for importert drivstoff [139]. Det er usikkert hvordan et globalt bortfall av GNSS vil påvirke globale maritime transportruter, men som i kapittel 5.1.6 vurderes det at trafikkflyten til sjøs vil tilpasses etter en lengre periode uten GNSS. På grunn av mangel på data er det også usikkert hvorvidt produksjonsanlegg, IoT for lagring og distribusjon og IKT-løsninger for pumping er avhengig av tidssynkronisering fra GNSS. Dermed er det også usikkert hvor stor evne de har til å motstå både korte og lengre forstyrrelser.

5.1.3 Ekomtjenester

Kommunikasjon er viktig for hele samfunnet, men kan få større betydning under kriser og krig, der viktig informasjon må nå ut til befolkningen og mellom myndigheter. Svikt i elektroniske kommunikasjonssystemer kan ramme andre samfunnsfunksjoner og dermed også totalforsvarets

funksjonsevne [129]. Å kunne opprettholde tilstrekkelig kommunikasjon mellom beredskapsaktører, styresmakter og innbyggere er avgjørende for blant annet evakueringer [144], og derav evnen til å håndtere ukontrollerte forflytninger av mennesker.

Sårbarheter

Vi vurderer at de landsdekkende ekomnettene er middels sårbare overfor forstyrrelser eller bortfall av GNSS.

I kapittel 3.2 beskrev vi at nøyaktig tids- og frekvenssynkronisering har stor betydning for mobilnettet, og særlig for å håndtere stor trafikk. Nøyaktigheten som trengs, oppnås med både GNSS-synkroniserte klokkekilder og egne atomklokker og varierer i sektoren. Telenor har for eksempel egne cesiumklokker i sin tidsinfrastruktur. Mobilnett er basert på en rekke standarder for tidssynkronisering, og det er viktig med sikker og nøyaktig tid. Det finnes også telekomspesifikke standarder for bruk av PTP og robusthet, men standardene spesifiserer ikke alltid løsninger, og konfigurasjoner vil variere blant aktører. Mobilnett er utviklet med noe grad av redundans (holdoverevne) som ikke nødvendigvis trenger kontinuerlig tilgang til GNSS. Derimot er GNSS fortsatt en integrert del av synkroniseringen for det norske mobilnett.

Konsekvenser

Vi vurderer at kortvarig jamming av GNSS vil få små konsekvenser for ekomtjenester. Det er derimot moderat usikkerhet for vurdering av konsekvenser som følge av mottak av forfalskede tidssignaler og et omfattende og langvarig bortfall, noe som vi vurderer kan få moderate konsekvenser.

De tidssensitive funksjonene til 4G- og 5G-nettene bidrar til økt tjenestekvalitet. Om det skulle oppstå noe avvik i tidssynkronisering, vil det fortsatt være mulig å bruke mobilnett til samtaler og kommunikasjon, men med redusert kvalitet (forstyrrelser eller lavere dekning). Tidsavvik kan derfor gå utover tjenestekvaliteten, men det vil ikke føre til fullstendig tap av funksjonen.

Det bør nevnes at ekomsektoren kan bli utsatt for andre typer RFI, eller elektromagnetisk krigføring, som også må kunne håndteres i kriser eller krig. Under krigen i Ukraina har RFI påvirket mobiltelefonsystemer og 5G direkte, noe som påvirker kommunikasjon mellom basestasjoner og terminaler, opplyser Telenor i sin rapport om digital sikkerhet [145]. Dette skjer i tillegg til jamming av GNSS-signaler, som kan påvirke tidssynkroniseringen [145].

5.1.4 Vannforsyning

Vannforsyning har stor betydning for liv og helse og er en viktig del av akutte helsetjenester og nødetatenes arbeid [129]. Vannforsyning spiller også en viktig rolle i Forsvarets vannbehov og sanitære behov [146], og NATO stiller blant annet krav til medlemsland om robust vannforsyning. Fungerende og veldimensjonert vannforsyning har også betydning for å kunne håndtere alliert mottak.

Sårbarheter

Vi vurderer at vannforsyningen har lav til middels sårbarhet overfor forstyrrelser eller bortfall av GNSS.

I likhet med kraftforsyning er vannforsyningssystemer avhengige av driftskontrollsystemer til overvåkning, styring og analyse av de ulike delene av systemet [147], og trenden går mot større grad av automatisering [148]. Slike systemer er avhengige av at utstyr har synkronisert tid for å fungere, som er beskrevet nærmere i kapittel 3.2.1.

I Norge er det 1 390 vannforsyningssystemer [149], og det finnes forskjellige leverandører og typer av driftskontrollsystemer. Veilederen til ett av systemene beskriver at interne klokke synkroniseres via NTP-server (*Network Time Protocol*, se kapittel 3) eller GNSS [150]. Under intervjuet diskuterte aktørene at NTP er mest sannsynlig den vanligste måten å synkronisere i slike systemer. NTP kan fortsatt være sporbart til GNSS, og vi vurderer sårbarheten knyttet til tidssynkronisering som moderat. Selv om driftskontrollsystemer er avhengige av tids-synkronisering har vi ikke avdekket strenge ytelseskrav til tidsnøyaktighet.

Automatisering og IoT-løsninger er utbredt i vannsektoren [148, 151]. Datainnsamling er i økende grad avhengig av IoT-sensorer og smarte vannmålere. SINTEF beskriver i en rapport stor variasjon i digitalisering blant kommuner og vann- og avløpsvirksomheter, og et stort antall leverandører av IoT-sensorer i Norge [151].

Posisjonsbestemmelse spiller en rolle for landmåling og kartlegging under vedlikehold og byggearbeid for vann- og avløpsanlegg. Det er mulig å utføre arbeidet med GNSS-uavhengig utstyr, men det kommer an på brukernes kompetanse og tilgjengelighet av utstyret. Dette ble vurdert som en sårbarhet under intervjudiskusjoner.

Konsekvenser

Vi vurderer at forstyrrelser og bortfall av GNSS vil få små konsekvenser for vannforsyningen.

Konsekvenser ved mulig tidsavvik vil avhenge av graden av digitalisering i hvert vannsystem og tekniske løsninger og aktørenes evne til å håndtere feil i synkronisering, og evne til å gå over på manuelle systemer. Ettersom vannforsyningen er lokal, er det lite trolig at bortfall av GNSS vil føre til konsekvenser på nasjonalt nivå.

5.1.5 Betalingssystemer

Finansielle tjenester tilrettelegger for at individer og bedrifter kan låne, spare samt gjennomføre betalinger og håndtere risiko [152]. Dette innebærer systemer som kontanter, betalingskort og girobetalinger samt aktivitetene i interbanksystemet. Fungerende betalingssystemer har stor betydning for stabiliteten i samfunnet og evnen til å utføre andre kritiske samfunnsfunksjoner. Robuste finansielle tjenester vil være avgjørende i kriser der rekvisisjonslovgivning ikke har trådt i kraft [9].

Sårbarheter

Vi vurderer at betalingssystemer har middels sårbarhet overfor forstyrrelser eller bortfall av GNSS.

Tidssynkronisering blant finansielle institusjoner som banker brukes til å tidsstemple betalings-transaksjoner. Finanssektoren har økt behov for nøyaktig tidssynkronisering for å kunne håndtere økende mengde transaksjoner. Handel som skjer på børsen, må følge strenge krav til nøyaktig tid, se kapittel 3.2.1. Lovverk om nøyaktighet (se tabell 3.3) og diskusjoner med aktører i finanssektoren viser til en viss robusthet i tidsnettverk for finansielle institusjoner. I dag tilbyr enkelte leverandører tidsnettverktjenester, men løsningene varierer blant aktører, hvor noen også utvikler egne nettverk med innebygd redundans, ifølge intervjudata.

Datagrunnlaget vårt er avgrenset til bank- og interbanksystemer og handel på børsen. Dog vurderer vi at betalingstjenester og andre digitale tjenester som BankID, Vipps, betalings-terminaler og minibanker er avhengige av tidssynkronisering. Det ble diskutert med aktører fra finanssektoren at økt bruk av sanntidsbetalingstjenester kan øke behovet for tidssynkronisering. For transaksjoner utover handel på børsen har vi ikke avdekket store krav til nøyaktighet, men integriteten i tidsstemplingen er viktig for å behandle transaksjonene.

Konsekvenser

Vi vurderer at lokale forstyrrelser av GNSS vil få små konsekvenser for betalingssystemer. Omfattende bortfall av GNSS kan få moderate konsekvenser, og vurderingen er forbundet med moderat usikkerhet.

På interbanknivå, det vil si systemene for overføring av penger mellom banker [153], har bruttotransaksjoner (enkeltbetalinger med verdi over 25 millioner kroner) større krav på nøyaktig tid enn nettobetalinger (avregninger), og begge er avhengige av tilstrekkelig tidssynkronisering i digitale nettverk. Avvik i tidsstemplene kan føre til forsinkelser i håndtering og utbetaling av betalinger ettersom det kan bli redusert oversikt og sporbarhet i transaksjoner. Evnen til å ivareta nøyaktighet avhenger av utstyret som brukes i de ulike systemene. Tidsavvik vurderes å ikke skape store konsekvenser for betalingstjenester mellom kundekontoer og banker.

Vi viser også til rapporten til Menon Economics som beskriver at betalingstjenester rettet mot forbrukere har indirekte avhengigheter til satellittbaserte eller innebygde klokke [10]. De vurderer at et 7-dagers bortfall ikke vil få store konsekvenser for samfunnskritiske områder som dagligvare, apotek og drivstoff.

5.1.6 Sjøtransport

Skipstrafikken står for den største andelen av varer som krysser over grensen. Trafikken øker stadig, og særlig med tyngre fartøy som tankskip og store cruiseskip [129]. Norske havner har stor betydning for alliert mottak [154]. Dersom enkelte havner må stenges for sivil trafikk i en krigssituasjon, vil den øvrige sivile sjøtrafikken måtte omdirigeres til andre havner som dermed får økt belastning [154]. Norsk sjøfart er i seg selv en kritisk samfunnsfunksjon. Samtidig er den en viktig del av den sivile støtten til militære operasjoner, og er avgjørende for å opprettholde andre viktige samfunnsfunksjoner som forsyning av mat og drivstoff [139].

Sårbarheter

Vi vurderer at sjøtransport har middels sårbarhet overfor forstyrrelser og bortfall av GNSS.

Det er mange systemer i sjøtransporten som er direkte avhengige av GNSS. Fartøy har gjerne flere navigasjonshjelpemidler i tillegg til GNSS, som også er påbudt å ha i større skip. Forskriften om navigasjonshjelpemidler for skip, det vil si passasjerskip og fartøy lengre enn 24 meter, beskriver utstyr som er påbudt, slik som gyrokompass, radar og ekkolodd i tillegg til GNSS [155]. Bruken av satellittnavigasjon til posisjonsbestemmelse blir enda viktigere når man beveger seg lengre ut fra kysten hvor navigasjonsradaren ikke har dekning til land og man mister fyrtårn av syne. Forskriften krever også å ha et elektronisk navigasjonskart eller ECDIS (*Electronic Chart Display and Information System*) med reservesystem (for eksempel papirkart) om bord i større skip. ECDIS-systemet bruker GNSS sammen med data fra blant annet ekkolodd, radar og gyrokompass [156]. GNSS benyttes også i stor grad for dynamisk posisjonering og i spesielle losoppdrag som større lekterforflytninger og dokkinger [106]. I en rapport utarbeidet av Royal Institute of Navigation i 2026 ble det også avdekket flere skjulte avhengigheter til GNSS. Basert på deres kartlegging kan flere systemer som i utgangspunktet ikke trenger GNSS, som både radar og gyrokompass, påvirkes av GNSS-forstyrrelser [157].

FNs internasjonale sjøfartsorganisasjon (IMO) stiller krav om ytelsen til GNSS-utstyr om bord på skip som også innebærer krav til integritetsovervåkning, slik som RAIM¹⁷ [158]. Nødpeilesendere benytter i økende grad GNSS-satellitter til peiling, i tillegg til andre signaler fra både LEO- og GEO-satellitter.

AIS (automatisk identifikasjonssystem) er også påbudt på større skip og brukes blant annet som antikollisjonssystem. GNSS står for posisjonsinformasjonen i AIS-meldingen, som kringkastes sammen med annen dynamisk informasjon om skipets identitet, fart og kurs. GNSS er avgjørende for posisjonsnøyaktigheten i AIS [159].

Sårbarheten øker lengre fra kysten utenfor rekkevidden av faste navigasjonshjelpemidler som radiofyr¹⁸. Lav sårbarhet ved forstyrrelser i GNSS forutsetter at navigatører har tilstrekkelig kompetanse i å navigere visuelt og kunne bruke GNSS-uavhengige navigasjonsmetoder og utstyr som radar. Under intervjuene kom det frem at navigatører i prinsippet ikke skal stole på kun GNSS-posisjon. Derimot vurderer vi at det kan være behov for å undersøke hvordan navigatører og utsyr på fartøy håndterer GNSS-forstyrrelser, særlig med økt bruk av GNSS.

Fremtidens autonome skip vil i stor grad være avhengige av fungerende GNSS sammen med interne treghetsnavigasjonssensorer [161, 162]. Økt bruk av autonome skip kan derfor føre til økt GNSS-avhengighet og dermed øke sårbarheten til funksjonsevnen for sjøtransport.

Konsekvenser

Vi vurderer at kortvarige og lokale forstyrrelser av GNSS vil få små konsekvenser for sjøtransport, men konsekvensene for sjøtrafikken er størst i områder med mye trafikk, som i store havner og trafikkfette transportruter. I tillegg vurderer vi at spoofing kan skape farlige situasjoner. Omfattende bortfall av GNSS kan få moderate konsekvenser for sjøtransport der funksjonsevnen

¹⁷ Receiver Autonomous Integrity Monitoring (RAIM) er en funksjon i GNSS-mottakeren som vurderer satellittdataenes troverdighet basert på målinger av mange satellittsignaler.

¹⁸ Radiofyr har vanligvis en rekkevidde på omtrent 70 nautiske mil [160]

reduseres i starten, men etter hvert som sjøfarten tilpasses situasjonen kan funksjonsevnen økes igjen. Allikevel vil kapasiteten være redusert sammenlignet med dagens tilstand.

Bruk av AIS og satellittdata har også betydning for maritim situasjonsforståelse og maritim sikkerhet (se boks 5.1). Bortfall av GNSS vil føre til reduksjon i overvåkingsevne og situasjonsforståelse. Dette kan få konsekvenser for trygg seilas og øke muligheten for ulovlig aktivitet – noe som svekker maritim sikkerhet.

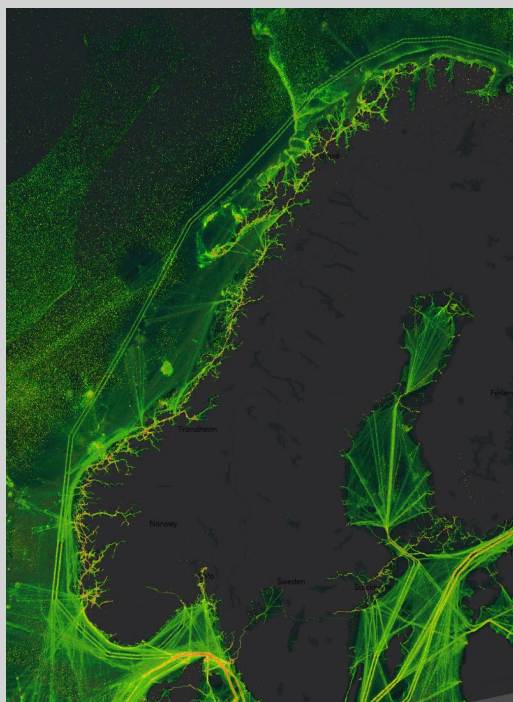
I 2025 og 2026 har det vært omfattende RFI i Hormuzstredet på grunn av geopolitisk konflikt og krig i området, noe som har gjort det utfordrende å navigere, særlig om natten [163]. Om et skip ikke oppdager at GNSS har falt bort eller viser feil posisjon, kan det føre til farlige situasjoner. I tillegg vil bortfall av GNSS føre til redusert effektivitet i transportflyten. Et gresk rederi rapporterte at de måtte redusere seilas gjennom stredet med 20 % [164], og myndigheter i Qatar satte restriksjoner på all sjøtransport i flere dager på grunn av GPS-feil [165]. GPS-forstyrrelser ble vurdert som årsaken til grunnstøting av containerskipet MSC Antonia [166].

Tap av GNSS kan skape usikkerhet og kreve at andre løsninger må tas i bruk for trygg navigasjon i sjøfarten. Navigasjon i varierende værforhold er dog en del av hverdagen, og det er etablerte og lange tradisjoner med manuelle navigasjonsmetoder, noe som ble understreket av intervju-deltakere. Mangel på posisjonsdata i AIS-meldinger og bruk av manuell navigasjon kan bety redusert fart for å navigere og ivareta sikkerheten. Det vil fortsatt være mulig å oppdage skip via radar og visuelle observasjoner.

Sjøfarten skal i utgangspunktet kunne opprettholde funksjonsevnen ved GNSS-forstyrrelser, men må regne med redusert hastighet for å ivareta sikkerheten. Ved et langvarig bortfall skal trafikken gradvis kunne økes igjen ved å ta i bruk andre systemer for å opprettholde nødvendig funksjonsevne, men med fortsatt lavere effektivitet enn normalt. Dette kan føre til lengre ledetider i transportruter og hos havner, og særlig i områder med høy trafikk.

Boks 5.1: Romvirksomhet øker maritim situasjonsforståelse

Satellitter har stor betydning for overvåking av skipstrafikk ved at de kan oppdage og forhindre ulovlig aktivitet, som ulovlig fiske [167], transport og omlasting av sanksjonerte varer [168], sabotasje [169] og spionasje [170]. AIS er en viktig komponent i arbeidet [171, 172]. BarentsWatch, som utviklet karttjenester knyttet til hav og kyst, bruker blant annet AIS-data og annen geodata for å skape et felles situasjonsbilde. Ser for eksempel figur 5.2.



Figur 5.2 Skjermbilde fra BarentsWatch som viser aggregert skipstrafikkdata fra AIS¹⁹.

Noen skip skruer av AIS-utstyret eller jammer sitt eget GPS-signal for å skjule seg [173]. Dette er en stor utfordring med tanke på for eksempel å hindre transport av sanksjonerte varer via Russlands skyggeflåte. Norge har mikrosatellitter fra før som utvider AIS-dekningen og bidrar til å overvåke havområdet med annen sensorikk, som radardetektoren på den norske NorSat-3, utviklet av FFI [174]. Lavlyssensoren på NorSat-4, utviklet av FFI, styrker evnen til å oppdage skip uten AIS ved bruk av lavlyskamera [175].

¹⁹ <https://www.barentswatch.no/arealverktoy/>

5.1.7 Veitransport

Veitranportressurser, både kjøretøy og veiinfrastruktur, har stor betydning for sivilbefolkningens og Forsvarets fremkommelighet og forsyningssikkerhet. Nødetatene trenger også fungerende veitransport, og bilambulansetjenesten er beskrevet som ryggraden i den prehospitale beredskapen i Norge. Dette diskuteres nærmere i kapittel 5.2.11. Totalberedskapskommisjonen beskriver at betydningen av veitransport for forsyninger over grensen har økt, og at opprettholdelse av transportflyt gjennom utenlandske korridorer er avgjørende i større kriser og krig [129]. Fungerende veitransport er viktig for evakueringer og derav evnen til å håndtere ukontrollerte forflytninger av mennesker.

Sårbarheter

Vi vurderer at veitransport har middels sårbarhet for forstyrrelser og bortfall av GNSS.

GNSS brukes i stor grad i kjøretøy til navigasjon. I tillegg bruker entreprenører posisjonstjenester fra GNSS for å gjennomføre byggearbeid og kartlegge utført arbeid. Det brukes også i digitale tjenester til datalagring og fakturering, noe som ble diskutert under intervjuene.

Behovet for nøyaktig posisjonsbestemmelse blant veibrukerne vil øke med økt digitalisering, for eksempel intelligente transportsystemer (ITS). Digitalisering i veitransporten betyr at data mellom kjøretøy, infrastruktur, og andre sensorer er brukt til for eksempel trafikkstyring, drift, vedlikehold og automatisering. Dette skal forbedre fremkommelighet, redusere utslipp og øke sikkerheten [176]. I Norge finnes det lov om ITS, men ingen forskrifter, og ifølge intervjuene spiller ikke GNSS en stor rolle for trafikkstyring i ITS i dag. Dersom slike systemer blir tatt i bruk i større grad, vil nøyaktig posisjon og tidssynkronisering være avgjørende for å ivareta ITS-funksjonene.

Konsekvenser

Vi vurderer at kortvarige og lokale forstyrrelser av GNSS vil få små konsekvenser for veitransport. Ved alvorlige kriser og krig kan det bli press på transportressurser. Dette kan øke behovet for å flåtestyre transportressurser for å opprettholde mest mulig effektiv veitransport. I slike situasjoner kan langvarig og omfattende bortfall av GNSS få moderate konsekvenser for veitransporten.

Evnen til å ivareta veiinfrastrukturen er avhengig av kontakt med entreprenører og ressurser som er tilgjengelig i området [129]. Store kriser og krig kan utfordre tilgjengeligheten av ressurser og skape samtidighetsbehov hos entreprenører. Mulig mangel på kompetanse og tilgang på GNSS-uavhengig utstyr for å utføre entreprenørarbeid kan være en utfordring ved bortfall av GNSS. Dette bør aktørene kartlegge for å få bedre forståelse av sårbarheten. Det ble også diskutert i intervjuet og i litteraturen at mangel på navigasjon og lokalisering for brøytearbeid kan få konsekvenser i form av forsinkelser eller arbeid som ikke blir utført under tilfeller av ekstremvær [177].

Mangel av eller feil posisjon i navigasjonssystemer i kjøretøy kan skape usikkerhet og flaskehalser i veitrafikken når problemene oppstår, men ved lengre bortfall kan det forventes at trafikken omstilles for å gjenopprette trafikkflyt.

5.1.8 Jernbanetransport

Jernbanen er sentral for forsyningssikkerhet og persontransport lokalt, regionalt og nasjonalt [129]. Jernbane er en viktig del av vertslandstøtte [178], og jernbanestrekninger ved alliert mottak vil være viktige forbindelsesakser for forflyttelse av styrker [138].

Sårbarheter

Vi vurderer at jernbanetransport er middels sårbar overfor forstyrrelser eller bortfall av GNSS.

I dag er posisjonen til et tog kjent basert på sensorer i bakkeinfrastrukturen (som baliser og akseltellere). Posisjonsangivelse via GNSS har en effektiviseringsrolle for trafikkstyring og for oversikt hos kunder, men har ikke en sikkerhetsfunksjon, basert på vår diskusjon med jernbaneaktører. GNSS-basert posisjonsbestemmelse kan spille en større rolle for styring av jernbanetrafikken ved introduksjonen av førerløse tog og ERTMS nivå 3. ERTMS (European Rail Traffic Management System) er et nytt system som innføres for styring av jernbanetrafikken på tvers av europeiske land.

Kartleggingen, både fra litteraturen og diskusjoner med sektoraktører, har identifisert behov for GNSS som støtte til overvåking og vedlikeholds- og byggearbeid for jernbaneinfrastruktur. Dette er både i form av innmåling og i form av innsamling av geodata for å kartlegge tilstanden i infrastrukturen via målevogn, der GNSS stedfester dataene som registreres.

Drift av jernbanen er avhengig av IKT-infrastruktur for styring og kontroll. I intervjuet ble behovet for synkronisering i fjernstyring av strømforsyningen og drift av jernbanens mobilnett (GSM-R) diskutert. Behovet for synkronisering i førstnevnte er viktig for hendelseslogging, feillokalisering og koordinering av operasjoner for trafikkstyring. Bane NOR opplyser at de har egen redundant infrastruktur for synkronisering med referanser fra GNSS (Galileo og GPS) og atomklokker.

Sårbarheten kan øke ved fremtidens bruk av GNSS til posisjonsbestemmelse og oppgradering av mobilnettet, se boks 5.2.

Boks 5.2: Fremtidens signal- og trafikkstyring for jernbanen

I dag er GSM-R en viktig ressurs for kommunikasjon mellom lokomotivførere, togledere og driftspersonell og har både nødansrop- og kringkastingsfunksjon [179]. ERTMS vil øke automatisering og digitalisering i trafikken og kreve oppgraderinger av GSM-R-systemet, basert på EU-standarden FRMCS (Future Railway Mobile Communications System). FRMCS-standarden blir basert på 5G-teknologi, og Norge blir forpliktet til å innføre den gjennom EØS-avtalen [180]. På ERTMS nivå 2 vil trafikksignaler kommuniseres via GSM-R istedenfor optiske signaler. På ERTMS nivå 3 blir Train Integrity Monitoring System (TIMS) introdusert, der posisjon fra GNSS blir brukt til å overvåke togintegritet (at toget er komplett med alle vogner) og for å posisjonere toget via bruk av virtuelle baliser.

Konsekvenser

Vi vurderer at kortvarige og lokale forstyrrelser av GNSS vil få små konsekvenser og at omfattende bortfall av GNSS kan medføre moderate konsekvenser. Denne vurderingen er forbundet med moderat usikkerhet.

Ved hendelser eller alvorlige ulykker vil tidsstemplet data fra distribuerte noder være viktig for å kunne lokalisere, løse og rette på feilen. I tillegg bidrar tidssynkronisering til trafikkstyringssystemet. Evnen til å håndtere tidsavvik vil komme an på konfigurasjoner hos ulike IKT- og synkroniseringsløsninger i jernbanesektoren.

5.1.9 Lufttransport

Luftfarten er en viktig del av norsk beredskap. Forsvaret er avhengig av sivil luftfart til transport av både eget og alliert personell og materiell [129]. Samarbeid mellom sivile aktører og Forsvaret er viktig for å sikre luftfarten, og det muliggjør NATO-operasjoner i norsk luftrom [129]. Luftfarten har blant annet stor betydning for nødetatenes evne til å håndtere masseskader og utføre akutte helsetjenester, som diskutert i kapittel 5.2.11. Luftfartens evne til å motstå forstyrrelser i hele krisespekteret er en viktig del av dens funksjon i totalforsvaret.

I luftfarten gjelder regelverk utarbeidet av EUs europeiske flysikkerhetsbyrå (EASA). I tillegg følges standarder og anbefalinger fra FNs internasjonale organisasjonen for sivil luftfart (ICAO) og lufttrafikkorganisasjonen Eurocontrol. Innenfor både navigasjon, overvåking og kommunikasjon forholder luftfarten seg til de tekniske standardene beskrevet i Annex 10 av ICAOs *International Standards and Recommended Practices*.

Sårbarheter

Vi vurderer at kommersielle luftfartstjenester er middels sårbare overfor forstyrrelser og bortfall av GNSS.

GNSS er en vesentlig del av navigasjonssystemer i luftfarten. Norge har et landsdekkende nett av bakkebaserte navigasjonshjelpemidler for underveisflyvninger. Fly er også utstyrt med GNSS-uavhengige systemer om bord i tillegg til GNSS til posisjonsbestemmelse. GNSS-uavhengige innflyvningssystemer hos mindre flyplasser bygges ned. Avinor beskriver at dette skal skje etter vurderinger som tar høyde for faren for GNSS-forstyrrelser [84]. Dette vil likevel øke avhengighet til GNSS. Det finnes alternativer og reserveløsninger for navigasjon, men ytelsesbasert navigasjon (PBN) som effektiviserer utnyttelsen av luftrommet er basert på nøyaktig posisjon fra GNSS.

I luftfarten kringkastes blant annet flyets GPS-posisjon via transpondersystemet ADS-B²⁰ (eller luftfartsradiosystem) til lufttrafikkjenesten for overvåking av trafikken. I 2023 ble installasjonen av WAM²¹ fullført, et system som til dels skal erstatte radarsystemer på bakken [181]. I Luftfartstilsynets navigasjonsstrategi beskrives det at begge disse systemene er avhengige av GNSS for tidssynkronisering, og at WAM kan få problemer innen kort tid ved bortfall [182]. Diskusjonen vår med intervjudeltakere viser at WAM krever tidsnøyaktighet på nanosekundnivå for å fungere, og at GNSS er særlig viktig for WAM lokalisert på fjelltopper.

Det opplyses av aktører innen luftfart at overvåkingssystemene i ulik grad er sårbare ved bortfall av GNSS, både for tid og posisjon, men at overlapp i systemene gjør dem mer robuste. NTP-løsningen er tilstrekkelig for å synkronisere dataene mot UTC og distribuere dem, og Avinor har egne klokkenoder som gir redundans i systemet.

Digitalisering i luftfarten kan øke behov for tidssynkronisering, særlig ved innføring av fjernstyrte tårn [183]. Fjernstyrte tårn innebærer at flere flyplasser er styrt ved et sentralt kontrollsenter. Kommunikasjonsløsninger for digitaliserte tårn vil kreve tilstrekkelig tidssynkronisering, noe som ble påpekt under intervjuet med aktører fra luftfartssektoren.

Konsekvenser

Vi vurderer at kortvarige lokale GNSS-forstyrrelser gir små til moderate konsekvenser for lufttransport, mens langvarig og omfattende bortfall av GNSS kan gi moderate til høye konsekvenser sammenlignet med dagens funksjonsevne.

Forfalskede signaler som ikke blir forkastet, kan også skape farlige situasjoner – noe som er viktig å ta hensyn til, særlig med stadig utvikling av spoofing-teknologi. Systemer kan reagere på GNSS-forstyrrelser på uventede måter, noe som gjør vurdering av konsekvenser for enkelte flyvninger usikkert. I tillegg har fungerende luftfart betydning for liv og helse når det gjelder medisinsk evakuering og redningsoperasjoner, noe som er diskutert i kapittel 5.3.11.

Hver lufttrafikkjeneste skal ha en GNSS-beredskapsplan som kan støtte operasjoner om GNSS blir utilgjengelig. Ved lokale forstyrrelser kan et fly gå over til andre navigasjonsmetoder eller omdirigeres til andre områder uten forstyrrelser. Dette kan først og fremst skape forsinkelser og noe lavere kapasitet i luftrommet. Hvorvidt enkelte flyvninger må omdirigeres eller utsettes, vil

²⁰ *Automatic Dependent Surveillance – Broadcast*

²¹ *Wide Area Multilateration*

være avhengige av type utstyr og rutiner på fly og hos flyplasser og av værforhold, lokasjon og årstid, men vil føre til større arbeidsbelastning for piloter og flygeledere, ifølge intervjudata og litteratur [184, 185]. Forstyrrelser kan føre til at en flyvning ikke kan lande der og når den trenger å lande.

Et eksempel på påvirkninger av RFI er når Finnish Airlines stanset alle flyvninger til Tartu lufthavn i én måned i 2024. Lufthavnen er ikke utstyrt med GNSS-uavhengige systemer og har vært utsatt for GNSS-forstyrrelser som har ført til at fly har måttet snu [186]. Turkish Airlines har også rapportert at flyvninger til Beirut har måttet snu på grunn av GNSS-forstyrrelser [186].

Ved nasjonale eller globale forstyrrelser beskriver Avinor i sin PBN-transisjonsplan at det også vil bli forstyrrelser i overvåkings- og kommunikasjonssystemer [84]. Under større kriser og krig vil behov for kommersiell luftfart gå ned, og kritiske behov prioriteres [187]. Evne til å motstå forstyrrelser og bortfall av GNSS vil fortsatt være avhengig av de nevnte faktorene, og det er behov for å øke oppmerksomheten rundt sårbarhet for forfalskede signaler for både posisjon og tid.

Faren for spoofing ble diskutert av intervjudeltakere og i eksisterende rapporter og litteratur [184, 188]. I 2024 ble det rapportert at i en periode på en måned ble 41 000 flyvninger utsatt for spoofing globalt [189]. Effektene av både jamming og spoofing i fly kan også være små nok til at alarmer ikke utløses eller utløses kun etter en lenger periode med GNSS-forstyrrelser, noe som gjør det vanskelig å oppdage [184].

Luftfarten har redundante systemer, men det er fare for at systemer får forfalskede posisjoner på grunn av et spoofing-angrep. En studie, utført i 2024 med data fra 2022, beskriver hvordan GNSS-forstyrrelser vil påvirke sivil luftfart i varierende grad basert på faktorer som flymodell, utstyr, og geografisk område og vil stort sett føre til økt arbeidsbelastning [184]. Disse funnene er i samsvar med diskusjoner med norske fagekspertene. Studien fra 2024 peker også på spoofing som problematisk, noe også diskutert under våre intervjuer. I tillegg kan konsekvensene øke ved forstyrrelser som også rammer bakkeinfrastruktur og varer i lengre perioder. Ifølge diskusjoner med fagekspertene, kan bortfall av GNSS redusere kapasiteten i luftrommet betydelig for å ivareta sikkerheten.

5.1.10 Matdistribusjon

Svikt i matforsyningen kan få følger for liv og helse, og matforsyningen er avgjørende for befolkningens motstandsdyktighet og Forsvarets utholdenhet. Matvareforsyning innbefatter hele forsyningskjeden fra råvareproduksjon og matvareforedling til distribusjon og konsum av matvarer. Vurderingen vår er avgrenset til distribusjonsdelen av matvareforsyning, som inkluderer både lagring og transport av matvarer, både for import og nasjonal distribusjon. Bruk av GNSS til landbasert matproduksjon diskuteres i boks 5.3.

Sårbarheter

Vi vurderer at matvaredistribusjon er lav til middels sårbar overfor forstyrrelser og bortfall av GNSS.

Posisjon av transportmidler brukes til flåtestyring i logistikk sammen med navigasjonssystemer i transporttjenestene. GNSS er den vanligste kilden til posisjon i flåtestyring, ifølge intervju med en fagekspert. Flåtestyringssystemer for logistikk er viktige for å optimalisere ruter og leveransetid. Bruk av GNSS i transporttjenestene er sårbare for forstyrrelser i GNSS. Det står mer om dette i de forrige delkapitlene.

Matdistribusjon blir også i større grad automatisert. For eksempel er ASKO sitt regionallager i Sande semi-automatisert og inkluderer automatiserte systemer og roboter for å fordele og frakte paller mellom anleggene [190]. Høyteknologiske løsninger i lageret skal være mer bærekraftige og effektive. Vi har ikke kartlagt bruk av GNSS for tidssynkronisering hos norske matdistribusjonsaktører, men viser til litteraturen om synkronisering i industrielle kontrollsystemer og kravene til tidsnøyaktighet, se kapittel 3.2.

Boks 5.4: PNT i landbasert matproduksjon

Både landbruk, havbruk og næringsmiddelindustrien opplever større digitalisering og automatisering. Presisjonsjordbruk er en form for IoT og er et satsningsområde for norsk landbruk, som beskrevet i Jordbruksoppgjøret 2025 [191]. Presisjonsjordbruk integrerer et bredt spekter av sensorer for å styre ressurser og øke produktivitet, kvalitet, profitabilitet, bærekraft og produksjonskapasitet [192]. Slike systemer kan tilpasse gjødsling for å få mest optimal bruk av gjødselen eller brukes til å spore husdyr på beite [192]. I likhet med andre bruksområder for IoT vil det være behov for synkronisert tid blant sensorene. GNSS er særlig brukt i navigasjonssystemer og autostyring av traktorer. Autostyring av traktorer i presisjonslandbruket benytter data samlet inn av sensorer for å effektivisere kjøremønstre.

Konsekvenser

Vi vurderer at forstyrrelser og bortfall av GNSS vil få små konsekvenser for matvaredistribusjon. Denne vurderingen er forbundet med moderat usikkerhet. Logistikkoperasjoner blir mindre effektive dersom flåtestyring med sanntidsposisjonering faller bort, men vi vurderer at det ikke vil få store konsekvenser for distribusjonsevnen nasjonalt.

Konsekvenser ved bortfall av posisjonsbasert flåtestyring kan være forsinkelser eller feil i koordinering av distribusjon og logistikkoperasjoner. Dette kan bety lengre ledetider for leveranser av varer, særlig for globale logistikkoperasjoner for importerte varer, som diskutert i kapittel 5.1.6.

Basert på litteratur om betydningen av tidssynkronisering i industrielle kontrollsystemer kan dette føre til mekaniske feil eller lavere effektivitet i operasjoner [54]. Konsekvenser av avvik i tidssynkronisering vil komme an på konfigurasjoner hos aktører og evne til å omstille operasjoner, noe som også spiller inn i generelle risikovurderinger for digitalisering og automatisering.

5.1.11 Nødetater

Akutte helsetjenester omfattes av helseberedskapsloven og skal kunne håndtere situasjoner med masseskader – noe som er avgjørende for sivil støtte til Forsvaret og allierte i en krigssituasjon [9]. Vi diskuterer her evnen hos nødetatene til å reagere og håndtere nødssituasjoner i hele krisespekteret. Den evnen kan få konsekvenser for liv og helse, påvirke befolkningens generelle motstandsdyktighet og utfordre Forsvarets utholdenhet [138].

Sårbarheter

Vi vurderer at nødetater har middels til høy sårbarhet overfor forstyrrelser eller bortfall av GNSS.

I kriser og krig er funksjonsevnen til nødetatene avgjørende for evnen til å håndtere masseskadehendelser og andre livstruende situasjoner. De aller fleste lokaliseringssystemer for nødmeldinger benytter GNSS i noen grad, og dersom nødmeldingen suppleres med GNSS-posisjon forbedres nøyaktigheten betraktelig sammenlignet med peiling av en tradisjonell nødpeilesender. GNSS er også brukt til lokalisering av ressurser, både personell og transportmidler, og til navigasjon til og fra nødssituasjoner, både på land, vei og sjø.

Risiko for lufttransporten, beskrevet i kapittel 5.1.10, kan også påvirke nødetatene. Enkelte lufthavner har bygget ned sine GNSS-uavhengige systemer. Ved forstyrrelser av GNSS vil mulighet til å lande komme an på utstyr om bord og værforhold, diskutert i intervju med aktører innen luftfart og i Navigasjonsstrategien [182]. Dette kan få konsekvenser for medisinske evakueringer i visse regioner. Avinor beskriver i 2023 at flyplasser i områder utsatt for GNSS-forstyrrelser (Øst-Finnmark) kommer til å beholde konvensjonelle navigasjonshjelpemidler (GNSS-uavhengige) inntil videre [84].

For helikopteroperasjoner gjør GNSS-baserte innflyvning og utflyvningssystemer det mulig å fly med marginal sikt, noe som gjør operasjonene sikrere [193] og reduserer utrykningstiden [194]. Under Jammertesten i 2024 testet Norsk Luftambulanses hvordan utviklingshelikopterets deres Airbus H145 håndterte falske signaler. Luftambulansen opplyser at systemene oppdaget spoofingen og sluttet å fly på autopilot – som indikerer at systemet ikke lot seg lure [195].

Det nye nødnett skal baseres på 5G [196], noe som øker behov for nøyaktig tidssynkronisering²².

Konsekvenser

Vi vurderer at forstyrrelser og bortfall av GNSS kan få store konsekvenser for nødetater og direkte konsekvenser for liv og helse.

Ved tap av GNSS reduseres evnen til å styre og delegere ressurser på en effektiv måte, særlig under større kriser som også krever store ressurser. Diskusjoner med aktører fra nødetatene peker mot at det å ta i bruk alternative metoder og reserveløsninger til lokalisering og navigasjon som

²² Kapittel 6.36.1 i ETSI-standarden TS 22.261 beskriver anbefalinger for mobilnett til nødetater og behov for reserveløsninger for nettverket ettersom GNSS er en typisk løsning for synkronisering i 5G nett. Dokumentet anbefaler flere tiltak for «5G timing resilience» for å detektere feil og gå over på reserveløsninger.

regel er mer tid- og ressurskrevende²³. Evnen til å håndtere GNSS-forstyrrelser vil være avhengig av beredskapsplanene til de ulike aktørene.

Tap av nøyaktighet i posisjon, mangel på posisjon eller falsk posisjon kan øke responstiden til nødetatene. Det fører til reduksjon i funksjonsevnen, noe som kan gå utover liv og helse, særlig om ressurser rykker ut til feil sted. Det gjelder også om nødmeldinger kommer inn i feil rekkefølge og blir oversett som følge av for eksempel et spoofing-angrep. Robust funksjonsevne for nødetater er av særlig betydning for å håndtere masseskader i krise og krig.

Dagens kommunikasjonsløsning til nødetatene, Nødnett, er basert på TETRA-standard og blir i liten grad påvirket av synkroniseringsproblemer, ifølge diskusjon med fageksperter.

5.2 Oppsummering og diskusjon

I dette delkapitlet diskuterer vi hvilke risikoer GNSS-forstyrrelser medfører for totalforsvaret, basert på funnene fra sårbarhetsvurderingen og risikoanalysene av de utvalgte samfunnsfunksjonene. Vi identifiserer også seks sektorovergripende sårbarheter, diskutert i delkapittel 5.2.1. Disse belyser et behov for videre arbeid for å identifisere og avdekke skjulte sårbarheter hos samfunnsfunksjoner bredt.

5.2.1 Sektorovergripende funn

Basert på kartlegging av bruksområder, trusler og farer, intervjuene og risikoanalysen har vi identifisert sårbarheter og usikkerhetsmomenter som går på tvers av bruksområder, og dermed berører flere kritiske samfunnsfunksjoner. Fordi dette er sårbarheter og usikkerheter som er sektorovergripende, kan de gi konsekvenser for PNT-brukere i totalforsvaret.

- **Avhengighet til GNSS og få alternative PNT-løsninger:** I Norge er det svært få måter for nøyaktig synkronisering mot UTC, eller en nasjonal tidsskala som ikke er basert på GNSS²⁴. Det betyr at bruksområder med behov for nøyaktig synkronisering mot UTC oftest benytter GNSS som referanse. Bruksområdene hvor posisjon og navigasjon er viktige, benytter GNSS i stor grad, og i noen tilfeller er det få alternativer, særlig for lokaliseringsteknologi og effektiv innsamling av geodata. I tillegg er det regionale forskjeller for navigasjon uten GNSS. Dette gjelder for eksempel GNSS-avhengige flyplasser og havområder uten andre faste navigasjonshjelpemidler. Det ble også nevnt av informanter at mulig nedbygging og stans i vedlikehold av bakkebasert infrastruktur for GNSS-uavhengig PNT (som fastmerker) bidrar til denne sårbarheten.
- **Mangel på nasjonale regelverk og standarder for tidssynkronisering:** Lovverk om sikre tidskilder finnes for finanssektoren og kraftsektoren, men disse spesifiserer ikke

²³ Under forstyrrelser i Øst-Finnmark rapporterer Babcock, et selskap som opererer luftambulanser i Norge, at GPS-jamming i verste fall kan skape forsinkelser eller at hjelpen ikke rekker frem til pasienten. De har likevel ennå ikke opplevd at slike forstyrrelser har ført til at de ikke har kommet frem til pasienten [197]

²⁴ Ved spesielt behov kan aktører synkronisere direkte med Justervesenets klokke [42].

løsninger eller enkelte viktige forutsetninger, slik som krav til stabilitet og andre sikkerhetstiltak. Det finnes ikke nasjonale regelverk eller standarder for andre samfunnsfunksjoner. Dette skaper usikkerhet om hvorvidt samfunnsfunksjoner er forberedt på og kan motstå forstyrrelser i GNSS, særlig ved økt digitalisering og automatisering.

- **Uvisshet om konsekvensomfang av GNSS-bortfall, særlig knyttet til økt digitalisering og automatisering:** Behov for nøyaktig synkronisering øker, og GNSS er en løsning som ofte er enkel å implementere. Økt digitalisering ble nevnt av flere aktører som en trend som vil øke behov for tidssynkronisering. Det er dog viktig at denne utviklingen tar hensyn til sårbarhetene knyttet til GNSS.
- **Utilstrekkelig øving på PNT-bortfall:** Flere aktører ønsker flere øvelser med bortfall av PNT, som også inkluderer spoofing av både tid og posisjon.
- **Redusert kompetanse på og tilgjengelighet av GNSS-uavhengige posisjons- og navigasjonssystemer:** Dette følger av økt avhengighet til GNSS. Et eksempel er at dersom GNSS er standard verktøy for en landmåler, vil kompetansen om tradisjonelle GNSS-uavhengige verktøy kunne forsvinne.
- **Usikkerhet knyttet til hvorvidt GNSS-utstyr og mottiltak benyttes og fungerer for å motstå trusler og farer:** Jammertesten på Andøya har vist stor variasjon i hvordan GNSS-utstyr (mottakere og beskyttelsestiltak, som anti-jammeantennor og spoofing-deteksjon) reagerer på forstyrrelser. Jammertesten har for eksempel vist at GNSS-mottakere ofte krever manuell omstart etter et jamme- eller spoofing-tilfelle. Det kan også ta flere timer før utstyret fungerer som vanlig igjen. Usikkerhet rundt utstyrets evne til å oppdage forfalskede signaler ble lagt særlig vekt på av flere fagekspertene. I intervjuer gikk det også frem at multi-GNSS-mottakere er i ferd med å tas i bruk, eller burde tas i bruk, for å øke robusthet. Det er dog ikke kartlagt i hvor stor grad mottakere brukt i samfunnet bredt benytter seg av multi-GNSS, noe som reduserer sårbarhet overfor RFI.

Det er behov for videre og kontinuerlig kunnskapsutvikling blant aktører for å forstå sårbarheter og konsekvenser ved bortfall av GNSS. Dette diskuteres nærmere i kapittel 6. Digitalisering fører til økt behov for tidssynkronisering og avhengighet til GNSS. For flere samfunnsfunksjoner fører høyt antall tjenesteleverandører, aktører og anlegg til usikkerhet i omfang av bruk av GNSS og i hvilken grad redundans og beskyttelse i systemer fungerer.

5.2.2 Risiko for totalforsvarsevne

GNSS som en kilde til tid og posisjon har forbedret funksjonsevnen til flere samfunnsfunksjoner, både i form av tilgjengelighet, omfang og effektivitet til PNT-bruksområder. GNSS er en lett tilgjengelig måte å synkronisere systemer på distribuert over et stort geografisk område, uten fysiske koblinger, og det tilrettelegger for digitalisering. For navigasjon har GNSS økt sikkerheten og effektiviteten ved å tilby en tjeneste med høy grad av tilgjengelighet, nøyaktighet, kontinuitet og integritet. GNSS til lokalisering har forbedret reaksjonsevnen til nødetatene betydelig. Studien viser at forstyrrelser i GNSS vil redusere funksjonsevne hos samfunnsfunksjoner sammenlignet

med dagens funksjonsevne. Økt og økende bruk av GNSS fører dermed til risiko for totalforsvarsevne, særlig gitt de identifiserte sårbarhetene.

I tabell 5.2 og 5.3 oppsummerer vi risikovurderingene for hver samfunnsfunksjon. Vi vurderer at de fleste samfunnsfunksjonene har middels sårbarhet overfor forstyrrelser eller bortfall av GNSS og nødetatene har middels til høy sårbarhet.

Vurderingen er basert på dagens tilstand, og økt digitalisering og bruk av GNSS vil øke sårbarheten om arbeid med redundans ikke skjer samtidig.

Vi har identifisert bruk av GNSS i alle samfunnsfunksjoner og funnet noen grad av redundans for å kunne håndtere i det minste kortvarige forstyrrelser i GNSS. Funksjonskritisk behov for PNT er i noe grad understøttet av redundante systemer, men kan fortsatt være sårbart for spoofing eller meaconing av signaler eller drift i interne systemer ved langvarig bortfall. Evnen til å håndtere eventuelt tidsavvik eller feil i posisjon avhenger av tilgang til og kompetanse om GNSS-uavhengige alternativer.

Vår vurdering er at tap av GNSS-signaler ikke vil føre til tidsavvik for de fleste tidskritiske funksjoner med en gang på grunn av «holdover»-evne og redundans. Det er derimot høy usikkerhet om konsekvensomfanget ved et spoofing- eller meaconing-angrep. Bruk av falske signaler kan skape konsekvenser også for tidskritiske funksjoner med innebygd redundans og vi har identifisert uvisshet om hvorvidt mottiltak klarer å motstå stadig mer avansert spoofing og meaconing.

Vi vurderer at det nasjonale mobilnett og kraftanlegg har en viss grad av redundans. Variasjon blant ekom-aktører og et høyt antall kraftaktører i Norge (for både produksjon og distribusjon) gjør denne vurderingen usikker. For vannforsyning har vi ikke identifisert et stort behov for nøyaktighet og vurderer at lokale vannforsyningssystemer vil være mindre sårbare overfor forstyrrelser i GNSS.

Bruk av GNSS til lokalisering og navigasjon har økt funksjonsevnen til nødetatene. Nødetatene har dermed høy sårbarhet overfor forstyrrelser i GNSS ettersom GNSS er brukt til posisjonsbestemmelse med lav redundans til flere funksjoner, noe som kan få alvorlige konsekvenser i form av tap av liv og helse. Nødetatene vil måtte benytte andre lokaliseringsmetoder og løsninger for flåtestyring og navigasjon som i mange tilfeller reduserer responstiden og øker arbeidsbelastning.

Forfalskede signaler er identifisert som en bekymring hos flere fageksperter, og vi vurderer at det er høy usikkerhet knyttet til konsekvenser ved et spoofing- eller meaconing-angrep – noe som da øker risikoen. Om falsk tids- eller posisjonsdata er brukt, kan samfunnsfunksjoner bli påvirket umiddelbart. Dette kan føre til farlige situasjoner i luft- og sjøfarten og stans i drift- og kontrollsystemer og digitale tjenester som bruker GNSS. For nødetatene kan feil eller mangel på posisjon i verste fall føre til tap av liv og helse.

Tabell 5.3 viser oppsummering av risiko for et omfattende bortfall av GNSS. Her vurderer vi at flere samfunnsfunksjoner kan oppleve moderate konsekvenser, det vil si et moderat tap av funksjonsevne. Dette kan være i form av driftsforstyrrelser i kraftsystemet, lavere tjenestekvalitet og kapasitet i mobilnettet, og forsinkelser og lavere kapasitet i transporttjenester – noe som kan gå utover logistikkoperasjoner og leveranser av forsyninger. I luftfarten vil konsekvensene være avhengig av regionale forskjeller og forskjeller blant operatører og fly – noe som kan bety både moderate og store konsekvenser for funksjonsevnen. Dette betyr redusert kapasitet til kommersiell luftfart og i noen tilfeller stans i flyvninger. Betalingssystemer kan få moderate konsekvenser i form g forsinkelser i håndtering av transaksjoner og terminaler som ikke fungerer men vi forbinder denne vurderingen med moderat usikkerhet.

Tabell 5.2 Risiko for at lokale og korte forstyrrelser av GNSS kan medføre alvorlige konsekvenser (svikt i funksjonsevne) for kritiske samfunnsfunksjoner.. Det er større usikkerhet knyttet til spoofing-angrep som kan øke risikoen.

Kritisk samfunnsfunksjon	Sårbarhet	Konsekvenser	Usikkerhet	Risiko
Kraftforsyning	Middels	Små	Moderat	Lav
Drivstofforsyning	Middels	Små	Moderat	Lav
Ekomtjenester	Middels	Små	Lav	Lav
Vannforsyning	Lav/middels	Små	Moderat	Lav
Betalingssystemer	Middels	Små	Lav	Lav
Sjøtransport	Middels	Moderate	Lav	Moderat
Veitransport	Middels	Små	Lav	Lav
Jernbanetransport	Middels	Små	Moderat	Lav
Lufttransport	Middels	Små/moderate	Moderat	Moderat
Matvaredistribusjon	Lav/Middels	Små	Moderat	Lav
Nødetater	Middels/Høy	Store	Lav	Høy

Tabell 5.3 Risiko for at omfattende bortfall av GNSS kan medføre alvorlige konsekvenser (svikt i funksjonsevne) for kritiske samfunnsfunksjoner.

Kritisk samfunnsfunksjon	Sårbarhet	Konsekvenser	Usikkerhet	Risiko
Kraftforsyning	Middels	Moderate	Moderat	Moderat
Drivstofforsyning	Middels	Moderate	Moderat	Moderat
Ekomtjenester	Middels	Moderate	Moderat	Moderat
Vannforsyning	Lav/middels	Små	Moderat	Lav
Betalingssystemer	Middels	Moderate	Moderat	Moderat
Sjøtransport	Middels	Moderate	Moderat	Moderat
Veitransport	Middels	Små	Lav	Lav
Jernbanetransport	Middels	Moderate	Moderat	Moderat
Lufttransport	Middels	Moderate/store	Moderat	Moderat/høy
Matvaredistribusjon	Lav/middels	Små	Moderat	Lav
Nødetater	Middels/Høy	Store	Lav	Høy

Nødetatene står overfor høy risiko ved et omfattende bortfall av GNSS. Bortfall, både kortvarige og langvarige, vil redusere effektivitet i krisehåndteringen og evnen til å håndtere masseskader. Flåtestyring og overvåking vil også være krevende ved bortfall av GNSS. I tillegg vil lokalisering av sivile ressurser under en krise, særlig i en krigssituasjon, være viktig for å unngå farlige og eskalerende situasjoner der sivile havner i farlige områder. Mulighet til å spore ressurser vil ha stor betydning for situasjonsforståelsen i krise og krig – også for at sivile transporttjenester kan navigere trygt for å ikke havne i farlige områder.

Mangel på evne til å motstå GNSS-forstyrrelser og ivareta funksjonsevne i hele krisespekteret reduserer motstandsdyktigheten i Norge og dermed totalforsvaret. Selv om enkelte funksjoner vurderes å ha lav eller middels sårbarhet, eller små til moderate konsekvenser, vil et scenario med nasjonalt bortfall av GNSS ramme alle aktører samtidig. Dette vil føre til kaskadeeffekter på tvers av samfunnsfunksjoner og samtidighetsbehov for ressurser som vil utfordre motstandsdyktigheten ytterligere. For eksempel vil forstyrrelser av GNSS-signalene øke faren for ulykker, som øker behov for redningstjenester og nødetater, som også selv vil ha redusert funksjonsevne.

Et omfattende bortfall av GNSS vil kreve tilgang til GNSS-uavhengige ressurser og kompetanse. Dette kan skje samtidig som konflikt og krig utsetter samfunnskritiske funksjoner for ødeleggelse og skaper stort samtidighetsbehov for både arbeidskraft og ressurser. Forstyrrelser i GNSS skaper også større arbeidsbelastning, for eksempel hos nødetater og luftfarten, noe som kan redusere situasjonsbevissthet, særlig i krisesituasjoner eller utfordrende navigasjonsforhold.

Økt hyppighet av ødeleggelse og cyberangrep mot infrastruktur vil øke behovet for rask feillokalisering og reparasjonsevne. Nøyaktig tidsbestemmelse, ofte sporbar til GNSS, er viktig for hendelseslogging i kontrollsystemer og feillokalisering i for eksempel strømmettet. GNSS brukt til landmåling og lokalisering av ressurser har også effektivisert reparasjonsarbeid. Vi vurderer at samtidighetsbehov for ressurser og arbeidsbelastningen som GNSS-uavhengig PNT krever, kan få konsekvenser for sivil støtte til militæret og opprettholdelse av kritiske samfunnsfunksjoner til befolkningen.

Studien har vært avgrenset til en vurdering av funksjonsevne til de utvalgte kritiske samfunnsfunksjonene, men det kan oppstå konsekvenser i samfunnet utover det som dekkes i vår risikovurdering. Kartleggingen av bruksområdene i kapittel 3 og sektorovergripende funn viser at flere sektorer og samfunnsfunksjoner enn dem vi har vurdert kan bli berørt av GNSS-forstyrrelser og bortfall. Dette inkluderer for eksempel posisjons- og navigasjonstjenester til landbruk, fiskeri og havbruk og lokalisering og geodata til forskning og miljøforvaltning. Droner benytter også i noe grad satellitt-tjenester til kommunikasjon og navigasjon, og de blir tatt i bruk i økende grad for å blant annet styrke situasjonsforståelse hos totalforsvarsaktører [198]. Droner brukes for eksempel til å overvåke kritisk infrastruktur, understøtte oppgaver til nødetatene og effektivisere reparasjonsarbeid. Dette bidrar til å styrke nasjonal forsvarsevne, men kan være sårbart for GNSS-forstyrrelser [198].

PNT og satellittvirksomhet bidrar til å øke Norges situasjonsforståelse. Tap eller forstyrrelser av tjenester kan skape usikkerhet i befolkningen og øke muligheten for ulovlig aktivitet eller for andre hybride trusler (se for eksempel boks 5.1). Norges lange kystlinje gjør oss sårbare for maritim fordekt etterretningsaktivitet, og i intervjuene var det bekymring for at bortfall av GNSS i et stort område kan øke handlingsrommet for ulovlig aktivitet. Totalberedskapsmeldingen beskriver maritim overvåking som et sentralt tiltak mot skyggeflåten, noe som innebærer økt tilstedeværelse og utbygging av satellitt- og dronekapasitet.

At GNSS er en integrert del av befolkningens hverdag, kan potensielt utnyttes av en aktør for å skape usikkerhet eller farlige situasjoner. I tillegg tilfører GNSS stor økonomisk verdi til samfunnet. Vi viser til rapporten til Menon Economics for en vurdering av samfunnsøkonomisk verdi som GNSS skaper [10].

Basert på sammensetningen av risiko for de ulike samfunnsfunksjonene og identifiserte sektorovergripende sårbarheter vurderer vi at GNSS-forstyrrelser eller bortfall medfører risiko for totalforsvarsevnen. Det vil si at dersom GNSS blir borte, kan det få konsekvenser for totalforsvarsevnen sammenlignet med dagens tilstand.

6 Risikoreduserende tiltak

GNSS har en iboende sårbarhet i den lave signalstyrken som gjør at alle brukere av GNSS kan være utsatt for både tilsiktede og utilsiktede forstyrrelser. Samtidig som denne studien har kartlagt bruksområder for satellittbasert PNT, har vi også identifisert flere sårbarheter. Under intervju diskuterte fagekspertene mulige sårbarhetsreduserende tiltak som oppsummeres i vedlegg C. For å identifisere aktuelle risikoreduserende tiltak brukte vi rammeverket til Critchley-Marrows og Verspieren [199], funnene om sårbarheter presentert i forrige kapittel og tiltakene identifisert under intervjuene og litteratursøk.

Critchley-Marrows og Verspieren sitt arbeid for å utvikle en felles forståelse av motstandsdyktig PNT (*resilient PNT*) definerer motstandsdyktighet som evnen til å gjenopprette eller fortsette operasjoner for å tilfredsstille kritiske behov, med en akseptabel reduksjon i funksjonsevne [199]. Rammeverket identifiserer fire hovedtemaer for å bygge motstandsdyktig PNT på nasjonalt nivå. Temaene består av å 1) karakterisere og vurdere, 2) forbedre og utvikle, 3) integrere og implementere og 4) samarbeide og koordinere. Sammen kan disse temaene oppsummeres som å forstå, utnytte, sikre og samhandle for motstandsdyktig PNT. Disse temaene er dekket av de anbefalte tiltakene.

De viktigste sårbarhetene identifisert i forrige kapittel er en avhengighet til GNSS, mangel på oversikt om avhengighet og bruk av GNSS til tidssynkronisering (noe som gjerne øker med økt digitalisering) og usikkerhet knyttet til beskyttelsestiltak og robusthet, i tillegg til øving og kompetanse. Dette forårsakes av mangel på nasjonale alternativer, mangel på nasjonalt regelverk og standarder og kompleksitet i bruken av GNSS.

Mangel på alternative tidsreferanser ble identifisert som en sektorovergripende sårbarhet. Flere totalforsvarsfunksjoner har økt sårbarhet ved lengre bortfall av GNSS på grunn av fare for klokke drift, også i egne redundante tidsnettverk. I tillegg kan GNSS signalet forfalskes, og det ble fremhevet i de forrige kapitlene usikkerhet rundt beskyttelsestiltak og konsekvensene av å ta i bruk feil tid eller posisjon. Under intervju ble det nevnt i diskusjoner med samtlige aktører som jobber med tidsnettverk, at bakkebaserte alternativer for tidsdistribusjon kan redusere sårbarheten knyttet til tidssynkronisering i Norge. Her ble det diskutert både utvikling av landsdekkende løsninger og økt samarbeid mellom aktører med egne tidsnettverk.

- Vi anbefaler å utvikle et nasjonalt bakkebasert alternativ for å ivareta en stabil tidsreferanse i Norge og Norges økonomiske sone. Samtidig bør muligheten for å utvide denne tjenesten til et PNT-system utredes.

Siden motstandsdyktig GNSS ikke fullt ut kan forhindre bortfall av GNSS, bør viktige samfunnsfunksjoner også benytte robuste multi-sensor PNT-systemer. Dette innebærer PNT-teknologier som er både støttende og alternative til GNSS, og som fungerer som redundans for GNSS. Eksempler på fremtidige PNT-teknologier er beskrevet i vedlegg B. Et robust multi-sensor PNT-system kan oppnås ved å anskaffe, utvikle og forske på alternativer til GNSS, enten satellittbasert eller bakkebasert.

-
-
- Vi anbefaler å satse på forskning, utvikling og innovasjon på robuste multi-sensor PNT-systemer.

GNSS skaper stor verdi hos sine brukere, kanskje særlig for totalforsvaret, og kommer til å fortsette å ha stor betydning for samfunnet. Samtidig er det identifisert at økt bruk av GNSS og mangel på tilgjengelige alternativer forsterker sårbarheten mot forstyrrelser. For å ivareta verdien skapt av GNSS og redusere risiko for bortfall bør bruken av GNSS gjøres mer motstandsdyktig. Dette inkluderer blant annet bruk av multi-GNSS-mottakere, anti-jammeantennener og støtte-sensorer til GNSS (som treghetssensorer og kamera). Med multi-GNSS-mottakere menes både multi-konstellasjon (utnytte alle GNSS-konstellasjoner) og multi-frekvens (utnytte alle GNSS-frekvensene). Tilgang til flere konstellasjoner gir tilgang til flere satellitter, noe som vil være viktig i områder der høye bygninger, dype daler eller bratte fjell skjærer for tilgangen til nok satellitter. I tillegg vil flere konstellasjoner gi tilgang til flere frekvenser. Mottakere som utnytter flere GNSS-frekvenser, vil kunne fungere dersom ikke alle frekvensene forstyrres samtidig. Et svært effektivt tiltak for å gjøre GNSS mer robust er å benytte anti-jammeantennener. Disse har evnen til å fjerne eller kraftig undertrykke jammesignaler fra et begrenset antall romlige retninger. Tidligere var denne typen antennteknologi hovedsakelig forbeholdt militært bruk, men den er nå også tilgjengelig for sivile brukere.

- Vi anbefaler å gjøre bruken av GNSS mer motstandsdyktig ved å ta i bruk for eksempel multi-GNSS-mottakere (multi-konstellasjon og -frekvens) og anti-jammeantennener.

Et annet viktig moment for å gjøre bruken av GNSS mer motstandsdyktig er å overvåke og varsle om GNSS-forstyrrelser. Dette krever at deteksjonsmetoder utvikles og kontinuerlig forskes på for å møte fremtidige RFI-trusler.

Risikoen, slik den er definert i denne rapporten, øker med usikkerheten i kunnskapsgrunnlaget om konsekvensene av GNSS-forstyrrelser og -bortfall. En måte å redusere usikkerheten på er å teste utstyret som brukes, i kontrollerte omgivelser. Jammertesten på Andøya er et eksempel på slike kontrollerte omgivelser. Her kan GNSS-utstyr som brukes i dag, eller som skal eller vurderes anskaffes, testes grundig for å tallfeste tålegrensene for jamming, spoofing og meaconing. Det at GNSS-signalet kan forfalskes utgjør også en økt risiko, særlig om beskyttelsestiltak ikke fungerer som det skal og feil tid eller posisjon blir brukt. Å teste utstyr blir et viktig tiltak for å gjøre bruken av GNSS mer sikker.

- Vi anbefaler at aktørene i totalforsvaret – særlig kritiske samfunnsfunksjoner som er avhengig av GNSS – tester utstyret sitt for å kartlegge sårbarheter i sine systemer. Vi anbefaler derfor også at det tilrettelegges for testing.

For deler av totalforsvaret som har behov for testing i mer lukkede miljøer, er egne tester for totalforsvaret et egnet alternativ.

For å redusere usikkerhet knyttet til robusthet, særlig ved økt bruk av GNSS, blir det viktig å utvikle PNT-retningslinjer i et nasjonalt rammeverk. Dette innebærer også at arbeidet og tiltak beskrevet i den nasjonale PNT-strategien fra 2018 følges opp og videreutvikles. Momenter

diskutert blant intervjudeltakere inkluderte å utarbeide sektorbaserte bestepsikser og behov for å kartlegge egne sårbarheter. For eksempel har Totalförsvarets forskningsinstitut (FOI) i Sverige publisert et dokument som beskriver metoder aktører kan bruke for å vurdere egne sårbarheter knyttet til GNSS i sammenheng med tid og frekvenssynkronisering [200]. Som beskrevet i boks 6.1 anbefaler rammeverket til USA (*Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture*) motstandsdyktighetsnivåer for ulike typer samfunnsfunksjoner [201]. Andre tilnærminger til nasjonal PNT-motstandsdyktighet er også beskrevet i boks 6.1

I våre diskusjoner om mulige tiltak med fageksperter kom det fram at øving på bortfall av PNT og integrering av dette i beredskapsplaner kan øke motstandsdyktigheten.. Krav til redundans, øving, testing i tillegg til mulige løsninger for robust PNT bør dekkes av et nasjonalt rammeverk – noe som bør baseres på et kontinuerlig oppdatert kunnskapsgrunnlag om sårbarheter og PNT-behov.

- Vi anbefaler å utvikle et nasjonalt rammeverk og retningslinjer for motstandsdyktig PNT og krav til samfunnssektorer om redundans.

For å styrke GNSS-tjenester i Norge bør vi fortsette å samarbeide med internasjonale miljøer for å forbedre sikkerheten og tilgjengeligheten av tjenestene. Sikkerheten kan for eksempel økes ved å benytte krypterte GNSS-signaler, noe som ble diskutert i intervjuene. Internasjonalt samarbeid er også viktig for å forhindre geopolitiske konflikter i verdensrommet. Utvikling av alternative PNT-systemer i rommet vil sannsynligvis kreve internasjonalt samarbeid. Dette er også viktig for å beskytte og sikre andre tjenester som leveres av satellitter, som kommunikasjon og jordobservasjon.

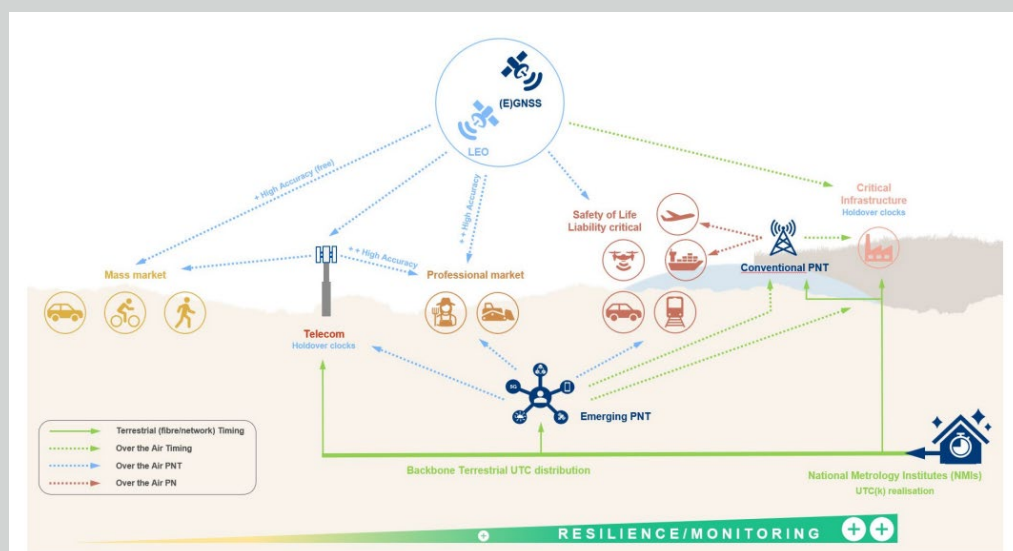
- Vi anbefaler å fortsette samarbeidet med internasjonale miljøer for å forbedre sikkerheten og tilgjengeligheten av satellittbasert PNT og andre satellitt-tjenester.

Boks 6.1: PNT-motstandsdyktighet i andre land

Flere land har identifisert nasjonale behov for motstandsdyktige PNT-systemer og har utviklet rammeverk for å oppnå dette. Slike strategier og rammeverk har som formål å sikre PNT-løsninger – både bakkebaserte og satellittbaserte.

I rammeverket til USA (*Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture* [201]) settes det et minimumskrav til PNT-motstandsdyktighet. Systemer som møter kravene til for eksempel nivå 1-motstandsdyktighet skal kunne gjenopprette funksjon etter at en forstyrrelse eller trussel er borte. Nivå 4 krever reserveløsninger som fører til at funksjonsevnen ikke reduseres i det hele tatt.

I 2023 utviklet EU en oppdatert versjon av European Radio Navigation Plan som beskriver hvordan GNSS kan bli introdusert i sektorspesifikke retningslinjer (*policies*) [202]. Her utvikles det planer for ulike typer behov kategorisert som massemarkedet, profesjonelt marked, kritisk for liv og helse eller for ansvar (*safety of life / liability critical*) og kritisk infrastruktur. Økosystemet for resilient PNT i EU vises i figur 6.1.



Figur 6.1 Modell av EUs målbilde for PNT fra [202].

Storbritannia har utviklet en PNT-strategi som også omfatter utvikling av nasjonal kompetanse på PNT, en spesifikk underetat for PNT hos Department of Science, Innovation, and Technology, en tverrsektoriell PNT-kriseplan og nasjonal tidsdistribusjon og FoU-plan for PNT [203].

7 Konklusjon

I denne rapporten har vi presentert PNT og satellittbaserte tjenester i Norge, beskrevet mulige tilsiktede hendelser og farer mot tjenestene og vurdert betydningen satellittbasert PNT har for totalforsvaret.

Det er flere utviklingstrekk som krever at PNT-motstandsdyktigheten i Norge styrkes. Satellittbasert PNT er i økende grad integrert i flere deler av samfunnet. Økt digitalisering og automatisering øker behovet for nøyaktige PNT-systemer til tidssynkronisering, noe som gjøres i stor grad med GNSS. Samtidig som det utvikles beskyttelsestiltak og sikkerhetstiltak for GNSS, foregår det også utvikling i systemer som kan slå ut eller lure GNSS. Stormakter styrker sine PNT-systemer²⁵, både satellittbaserte og bakkebaserte, samtidig som de tester anti-satellittvåpen. Norge opplever daglige GNSS-forstyrrelser fra Russland i Øst-Finnmark.

Vi har identifisert seks sektorovergrepene sårbarheter som bidrar til økt risiko for samfunnsfunksjoner og totalforsvaret. Disse er:

- avhengighet til GNSS og få alternative PNT-løsninger
- mangel på nasjonale regelverk og krav for tidssynkronisering
- uvisshet om konsekvensomfang av GNSS-bortfall knyttet til økt digitalisering og automatisering
- utilstrekkelig øving på PNT-bortfall
- redusert kompetanse på og tilgjengelighet av GNSS-uavhengig posisjons- og navigasjonssystemer
- usikkerhet knyttet til hvorvidt GNSS-utstyr (særlig multi-GNSS) og mottiltak benyttes og fungerer for å motstå trusler og farer

Evnen til å motstå forstyrrelser i hele krisespekteret for å sikre individenes sikkerhet og samfunnsverdier utgjør en viktig del av totalforsvaret. Satellittbasert PNT har gjort kritiske samfunnsfunksjoner tryggere og mer effektive. Vi har kartlagt omfattende bruk og nytte av GNSS og vurdert at det er risiko for at flere kritiske samfunnsfunksjoner kan få redusert funksjonsevnen ved bortfall av GNSS – noe som får betydning for samfunnets motstandsdyktighet og den sivile støtten til forsvaret. Dette betyr for eksempel forsinkelser i leveranser, forstyrrelser i kraftforsyning, mobilnett, og betalingssystemer, redusert evne til å håndtere masseskader og redusert situasjonsforståelse. Mangel eller feil i posisjon kan få konsekvenser for nødetatene som går utover liv og helse og skape farlige situasjoner for transporttjenester. Forfalskede signaler ved et spoofing- eller meaconing-angrep er vanskelig å oppdage og øker risiko for GNSS-brukere. I

²⁵ For eksempel jobber USA stadig med å oppgradere og styrke GPS [204], og Kina har også et omfattende bakkebasert nettverk for PNT som inkluderer eLoran [205].

tillegg vil systematiske sårbarheter i bruken av GNSS og dagens behov for PNT medføre risiko for flere bruksområder enn dem som er analysert.

I lys av totalforsvaret er det viktig at aktører innen kritiske samfunnsfunksjoner er bevisst på sine egne sårbarheter knyttet til både satellittbasert PNT og behovet for andre satellittbaserte tjenester. Erfaringer fra Jammertesten på Andøya har belyst flere sårbarheter som brukere kan ha uten å være klare over det. Egne kartlegginger og samarbeid på tvers av aktører og sektorer for å utveksle kunnskap og erfaringer blir viktig for å forstå og redusere sårbarhetene.

For å redusere sårbarheten hos GNSS-brukere i Norge har vi identifisert seks hovedtiltak (beskrevet i mer detalj i forrige delkapittel):

- tilrettelegge for og gjennomføre testing av utstyr for å identifisere og kartlegge sårbarheter
- utvikle nasjonale rammeverk og retningslinjer for PNT og krav til samfunnssektorer for redundans
- utvikle bakkebaserte alternativer for å ivareta en stabil tidsreferanse i Norge og Norges økonomiske sone
- gjøre bruken av GNSS mer motstandsdyktig
- utvikle robuste multi-sensor PNT-systemer
- fortsette med internasjonalt samarbeid for å forbedre sikkerheten og tilgjengeligheten av satellittbasert PNT

Tiltakene kan redusere sårbarheten og bidra til å forstå, utnytte og sikre PNT for å oppnå verdien av satellittbasert PNT og redusere risikoen ved bruk av GNSS. Tiltakene forutsetter videre kunnskapsutvikling og at både aktører og myndigheter kontinuerlig jobber med å utvikle og styrke PNT-løsninger i samfunnet i stort og innen ulike samfunnsfunnsområder.

Motstandsdyktig PNT og satellitt-tjenester er en viktig del av et velfungerende totalforsvar, og evnen til å motstå forstyrrelser får betydning i hele krisespekteret og i møte med sammensatte trusler. Dette krever kontinuerlig arbeid på tvers av sektorer og landegrenser for å sikre at samfunnet vårt kan fortsette å dra nytte av nye teknologier samtidig som vi er forberedt på å møte fremtidige utfordringer.

Vedlegg

A Metodisk tilnærming

A.1 Avgrensninger

Behov og bruk av PNT i Norge

Rapporten kartlegger behov for PNT og bruk av satellittbasert PNT. For å avgrense og systematisere kartleggingen ble sektorer og undersektorer identifisert basert på totalforsvarsfunksjoner fra rapporten *Sivil støtte til Forsvaret – en funksjonsbasert tilnærming for modellering av totalforsvarsevne* [206] med tilpasninger for å øke fullstendigheten i kartleggingen. Sektorene og undersektorer dekket i denne studien er beskrevet i Tabell A.1.

Vurdering av risiko for totalforsvar

Vurdering av risiko for totalforsvar er avgrenset til undersektorene påpekt i rapporten *Sivil støtte til Forsvaret – en funksjonsbasert tilnærming for modellering av totalforsvarsevne* [9]. Disse tilsvarende undersektorene i tabell A.1 unntatt de i kursiv.

Risikoanalyse er avgrenset til å vurdere funksjonsbaserte konsekvenser. Vurderingen er kvalitativ. Merk at det i intervjuguiden i delkapittel A.2.1 er beskrevet kvantitative vurderinger av konsekvensen. Dette ble brukt for å skape diskusjon, men de kvantitative vurderingene fra intervjuet er ikke brukt i risikoanalysen. Metode for risikoanalysen er beskrevet nærmere i kapittel 5.

A.2 Datainnsamling

Vi har kartlagt bruk av PNT i Norge ved å først ta utgangspunkt i eksisterende dokumenter og rapporter som inkluderer Norges PNT-strategi [207], Norsk romsenter (nå Direktoratet for romvirksomhet) sin GNSS-sårbarhetsanalyse *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur* [16], *Satellite-derived time and position: Blackett review* [14], London Economics *The economics impact on the UK of a disruption to GNSS* [15] og EUSPA sin markedsrapport for GNSS og EO (Earth Observation) [208].

For de utvalgte sektorene ble det også gjennomført et litteratur- og dokumentsøk for å identifisere bruksområder bredt i Norge. Et vedlegg med kartlagte bruksområder ble sendt til intervjudeltakerne og diskutert under semistrukturerte intervjuer og videre dialog for å fylle gap og verifisere for norsk kontekst samt bidra med faglig ekspertise om behov for PNT og mulige konsekvenser ved bortfall av satellittbasert PNT. Eksempler på søkeord inkluderer: GNSS, GPS,

PNT, synchronisation, timing, precise timing, positioning, navigation, synkronisering, tidsbestemmelse, posisjonsbestemmelse, navigasjon, og nøyaktig tidsbestemmelse.

Under kartleggingen ble bruksområdene kategorisert og spisset, og de beskriver følgende PNT-funksjoner: tidssynkronisering, lokalisering, landmåling, sanntidsovervåking, geodata og navigasjon.

Tabell A.1 Sektorer og undersektorer dekket i kartleggingen. Undersektorer i kursiv er ikke inkludert i risikovurderingen

Sektor	Undersektor
Energiforsyning	Forsyning av drivstoff
	Forsyning av elektrisk energi
Matvareforsyning	Matvaredistribusjon
	<i>Landbruk</i>
	<i>Fiskeri- og havbruk</i>
Vannforsyning	Vannforsyningssystem
Nødetater	Politiet
	Helsetjenester
	Brannvesenet
Ekomtjenester	Ekomnett
Transporttjenester	Veitransport
	Jernbanetransport
	Sjøtransport
	Lufttransport
Finansielle tjenester	Betalingsystemer
	Handelssystemer

Intervjudata er brukt for å kartlegge betydningen PNT har for samfunnsfunksjonene og for å vurdere konsekvenser ved bortfall av PNT. Informantene svarte på spørsmål om i hvilken grad et bortfall av PNT-funksjoner, som varer fra ett døgn til 30 dager, får konsekvenser for samfunnsfunksjonen. Et semi-strukturert intervjuformat gjorde at spørsmålene var åpne for diskusjon om forutsetninger og faktorer som påvirker konsekvensene, og om tidshorisont og virkemidler for bortfall (for eksempel spoofing eller jamming).

Antall deltakere og aktører varierte for de ulike sektorene og inkluderte aktører med erfaring innen PNT eller beredskap i sektoren. Deltakerne ble tilsendt intervjuguiden med spørsmål og kartlagte bruksområder for å gi mulighet til å samle informasjon i forkant av intervjuet. Intervjuet dekket tre hovedtemaer: (1) arbeid med og oppmerksomhet om PNT i sektoren og trender knyttet til det, (2) bruksområder og avhengigheter til PNT og (3) konsekvenser ved bortfall av satellittbasert PNT.

Vi gjennomførte intervjuer med 25 ulike norske aktører, både myndigheter og næringslivsaktører. Sektorene og undersektorene som ble dekket av intervjuene var:

- kraftsektoren
- ekom-sektoren
- havindustri
- finanssektoren
- logistikk (land og sjø)
- landbruk
- fiskeri- og havbruk
- vann og avløp
- nødetatene (brann, politi, ambulanse, nødnett)
- digitale helsetjenester
- veisektoren
- jernbanesektoren
- sjøtransport
- lufttransport

-
-
- romvirksomhet
 - karttjenester
 - tidstjenester

Deltakerne ble også spurt om forberedelsene gjort i forkant av intervju. Flere har tatt interne runder for å kunne dekke alle områder i intervjuet. Det ble også videre dialog med flere deltakere etter intervjuene for å kvalitetssikre og fylle gap fra intervjuet.

Begrensninger

Mulighet til å dekke alle bruksområder med norske fageksperter ble begrenset av ulike faktorer, og aktørene bidro med kunnskap om både virksomhetene sine og sektorene bredt. Intervjudata komplementerer data samlet inn fra faglig litteratur.

Intervjuguide

Følgende intervjuguide ble brukt for de første rundene av intervjuer med sektoraktører. I tillegg brukte vi en tilpasset intervjuguide til intervju med PNT-sektoraktører (aktører innen romvirksomhet, karttjenester og tidstjenester). I de intervjuene ble alle sektorene diskutert. En forkortet intervjuguide ble også brukt for supplerende intervjuer (andre runde) som dekket de tre hovedtemaene.

Innledning

Bakgrunn

Forsvarets forskningsinstitutt (FFI) jobber nå med en utredning om samfunnets avhengighet til satellittbasert posisjons-, navigasjons-, og tidsbestemmelsestjenester (PNT) på oppdrag for Nærings- og fiskeridepartementet. Samfunnets avhengighet av satellittbaserte tjenester og mangel på reserveløsninger har blitt utpekt som en strategisk sårbarhet for Norge i den åpne trusselvurderingen til NSM (Nasjonal Sikkerhetsmyndighet). I tillegg, finnes det ingen tilstrekkelig kartlegging av avhengighetene og betydning for totalforsvaret.

FFI har identifisert flere sektorer som har viktig samfunnsfunksjoner når det gjelder totalforsvar. I gruppeintervjuer med sektoraktører, ønsker vi å dekke tre kunnskapsbehov for å bidra til dataen for utredningen. Vi ønsker å skape en oversikt om arbeid eller mangel på arbeid rundt PNT i sektoren, kartlegge bruk av PNT-tjenester i sektoren, og få en ekspert vurdering om konsekvenser ved bortfall av satellittbasert PNT i sektoren.

PNT og GNSS

Den mest kjente løsningen for satellittbasert PNT er GPS (Global Positioning System). GPS er et amerikansk system av satellitter som distribuerer tid og

posisjonstjenester over hele verden. GPS er en av fire globale navigasjonssatellittsystemer (GNSS), sammen med russiske GLONASS, kinesiske BeiDou, og EUs Galileo. GNSS, satellittbasert PNT, er avhengig av synkronisert og nøyaktig tid for å beregne posisjoner av mottakere på bakken, og hver satellitt er rustet med en atomklokke. Det har derfor også blitt en viktig kilde for tidsbestemmelse på bakken. I tillegg til satellittbasert PNT, finnes det andre bakkebaserte og lokale PNT-løsninger. For eksempel, treghetsnavigasjon, WiFi-posisjonering, og bakkebaserte fibernettverk for tidsbestemmelse.

Generelle kapabiliteter styrket eller muliggjort ved bruk av PNT-tjenester kan kategoriseres som:

- Aktivitetssporing og operasjonsstyring
- Infrastruktureovervåking
- Lokasjonsbaserte tjenester
- Timing og synkronisering
- Navigasjon og posisjonering
- Forskning og analyse

Forberedelser til intervju

Vi ønsker at deltagerne bruker litt tid på å samle informasjon til svarene på intervju spørsmålene i forkant av intervjuet. Les gjennom intervjuguiden som ligger under, disse er spørsmålene som kommer til å bli stilt og diskutert under gruppeintervjuet.

Intervjudataene blir til slutt vurdert sammen med andre datakilder for å skape et helhetlig bilde. Vi setter også pris på henvendelser til andre kilder, datasett, virksomheter eller aktører som kan være nyttig for datainnsamlingen vår.

Intervjuguide

1. Arbeid og oppmerksomhet rundt PNT avhengigheter

Hensikt:

Identifisere mulige datakilder til kartleggingen av bruk av PNT

Identifisere usikkerhet og kunnskapsgap for videre arbeid

1.1 Finnes det en virksomhet eller person som har et spesifikt ansvar eller rolle innenfor PNT/GNSS i din sektor?

1.2 Finnes det standarder, lover, og/eller regelverk om bruk av posisjonstjenester eller tidsbestemmelse i en eller flere deler av din sektor?

1.3 Har bruk og/eller verdi av PNT/GNSS blitt kartlagt i din sektor eller hos din virksomhet?

1.4 Har PNT spilt en rolle i risikovurderinger i deler av din sektor? Enten for å redusere risiko eller som en sårbarhet?

1.5 Finnes det teknologiske trender/satsninger som gjør sektoren mer avhengig av PNT? For eksempel, autonome og intelligente systemer?

2. Bruk av PNT i sektoren

Hensikt: Å skape en forståelse om avhengighet av PNT tjenester i sektoren.

2.1 Hva er viktige avhengigheter til satellittbaserte PNT-tjenester i din sektor? Ta gjerne hensyn til listen av kapabiliteter muliggjort og styrket av PNT-tjenester.

2.2 Vi har samlet en liste av bruk av PNT i din sektor (se vedlegg), gjennom en litteraturgjennomgang. Hvordan samsvarer dette med norsk kontekst? Mangler det viktige avhengigheter?

3. Konsekvenser ved bortfall av satellittbasert PNT

Hensikt: Å få sektoreksperter sine kvalitative og kvantitative vurderinger av konsekvenser ved bortfall av satellittbasert PNT. Svarene skal settes sammen med andre datakilder for å senere gjøre en helhetlig konsekvensvurdering.

Vi ønsker å få en kvantativ²⁶ vurdering av konsekvenser ved svikt i PNT. Svikt kan bety både svikt i integritet, kontinuitet, tilgjengelighet, og/eller nøyaktighet. Vi bruker derfor en skala fra 0-5 for *konsekvensgrad*:

5: Tap av funksjonsevne betyr at det blir ikke mulig å utføre funksjonen hvis det ikke er tilgang til PNT-tjenester.

2-4: Degradering av funksjonsevne betyr at evnen er svekket. 2 betyr svekket i liten grad, og 4 er i større grad. Dette kan begrunnes av redundans i systemet, reserverløsninger, eller betydningen PNT har for selve funksjonsevnen.

1: Endret operasjonsmodus betyr at alternative løsninger er iverksatt, uten mye endring i funksjonsevne, men med en viss omstillingsperiode.

3.1 Hvilke deler av sektoren har de mest umiddelbare og kritiske konsekvenser for samfunnet hvis det er svikt i PNT i opptil ett døgn?

3.2 Hvordan benyttes PNT i de delene av systemet?

3.3 Basert på svarene i 3.1 og 3.2, hva er konsekvensgraden for funksjonen i de delene av sektoren ved bortfall i ett døgn?

3.4 Hvis PNT var borte i 30 dager, hva er konsekvensgraden for din sektors samfunnsfunksjon i sin helhet?

3.5 På kortsikt og langsikt, hva kan gjøres for å redusere sårbarheten og konsekvenser knyttet til avhengighet til satellittbasert PNT?

4. Avrundende spørsmål

Fortell om forberedelsene gjennomført i forkant av intervjuet.

Finnes det andre kilder (dokumenter, datasett, virksomheter, nøkkelpersoner) som kan være nyttig for oss?

Vi er også åpne for oppfølgingsmøter hvis dere vil komme med mer innspill.

Vi tar kontakt om det er behov for avklaringer, og for å ferdigstille dataene til rapporten.

²⁶ Merk at risikoanalysen i rapporten er ikke kvantitativ. Dette er beskrevet videre i avgrensninger.

A.3 Kriterier for risikoanalyse

Tabell A.2 Vurderingskriterier for sårbarhet

Sårbarhet	Kriterium
Høy	Høy avhengighet til GNSS med lav redundans (for eksempel mangel på reserveløsninger eller alternativer).
Middels	Bruk av GNSS med noe redundans (for eksempel reserveløsninger med redusert ytelse eller begrenset holdover-tid).
Lav	Lavt behov eller ingen strenge ytelseskrav til PNT. Bruk av GNSS med høy redundans (for eksempel reserveløsninger eller alternativer med samme ytelse).

Tabell A.3 Vurderingskriterier for konsekvenser

Konsekvens	Kriterium
Store	Stort tap av funksjonsevne eller at kun en viss funksjonsevne opprettholdes.
Moderate	Moderat tap av funksjonsevne.
Små	Lite eller ikke noe tap av funksjonsevne.

Tabell A.4 Vurderingskriterier for usikkerhet

Usikkerhet	Kriterium
Høy	Høy usikkerhet i kunnskapsgrunnlaget. Mer informasjon er nødvendig.
Moderat	Moderat usikkerhet i kunnskapsgrunnlaget. Resultatene bør brukes med forsiktighet. Mer informasjon kan være nødvendig for å kompensere for usikkerheten.
Lav	Robust kunnskapsgrunnlag. Mer informasjon er ikke nødvendig.

Tabell A.5 Vurderingskriterier for risiko

Risiko	Kriterium
Høy	Middels eller høy sårbarhet og potensial for store konsekvenser. Høy sårbarhet og potensial for moderate konsekvenser. Høy usikkerhet.
Moderat	Middels sårbarhet og potensial for moderate konsekvenser. Høy sårbarhet og potensial for små konsekvenser. Lav sårbarhet og potensial for store konsekvenser.
Lav	Ikke noe potensial for alvorlige konsekvenser, lav sårbarhet og lav eller moderat usikkerhet

B Alternativ og fremtidig PNT-teknologi

Vi definerer alternativ og fremtidig PNT-teknologi som løsninger som kan komplementere eller erstatte GNSS. I dette kapitlet presenteres både eksisterende teknologier som kan brukes i dag, og teknologi og løsninger som ligger lenger frem i tid. Et kunnskapsgrunnlag utarbeidet av en underleverandør fra *Institute for Security Science and Technology* på Imperial College London og AstraTerra har pekt på disse teknologiene som viktige deler av en PNT-arkitektur for å oppnå redundant og motstandsdyktig PNT.

B.1 LEO PNT

I dag finnes det over ti selskaper som utvikler dedikerte lavbanekonstellasjoner for å levere PNT-tjenester (LEO PNT) med planer om i overkant av 2 500 satellitter. Fem av disse selskapene har satellitter i rommet i dag og utgjør totalt rundt 50 satellitter. Selskaper som CentiSpace, Geely og SatNet LEO fra Kina leder an i skrivende stund med størst antall satellitter i bane. Xona Pulsar og TrustPoint fra USA, med henholdsvis to og tre satellitter, er selskaper som har fått mye oppmerksomhet i internasjonale GNSS-miljøer.

Fra Europa planlegger ESA å sende opp en demonstratorkonstellasjon bestående av 10 LEO-satellitter med PNT som hovedformål. Konstellasjonen har fått navnet Celeste, og har i 2026 sendt opp de første to satellittene. Alle de dedikerte PNT-konstellasjonene er planlagt med 200–500 satellitter hver, bortsett fra Celeste, hvor man trolig vil avvente resultater fra demonstratoren.

Dedikerte PNT-satellittkonstellasjoner i lav jordbane vil gi kraftigere signaler ned til bakken i og med at de er vesentlig nærmere enn GNSS-satellitter i mellombanområdet (MEO). Den økte signalstyrken og lavere høyde (vanskeligere for jammere å se satellittene) vil kunne øke motstandskraften mot jamming og gjøre innendørs satellittnavigasjon (som for eksempel i bygninger) mulig. For å ha tilnærmet samme dekning som GNSS kreves det mange flere satellitter i LEO enn i MEO. Selv om det har blitt svært mye billigere å sende opp små satellitter i bane, er det fortsatt en stor kostnad å utvikle, sende opp og drifte en LEO-konstellasjon.

Per i dag er det kun én annen konstellasjon som leverer PNT-tjenester utenom GNSS fra rommet. Iridiums tjeneste Satellite Time and Location (STL) kringkaster PNT-informasjon fra sine 66 kommunikasjonssatellitter. Disse satellittene er altså ikke dedikerte PNT-satellitter, men bærer med seg ulike nyttelaster, slik som STL. Tjenesten passer best for stasjonære mottakere grunnet signaltypen som brukes. Konstellasjonen har også relativt få satellitter sammenlignet med de planlagte dedikerte LEO-PNT-konstellasjonene. Posisjonsnøyaktigheten til denne tjenesten er ikke like god som GNSS, men kan fungere som komplement for fravær av GNSS for brukere med moderate krav til PNT. Iridium-satellittene går i polare baner som gir god dekning i nord. Signalene fra STL er om lag 1 000 ganger sterkere enn GNSS målt ved bakken, og er dermed mer robuste mot forstyrrelser. Frekvensen som benyttes, er ganske nær GNSS-signalene, og man kan ofte bruke samme antenner til begge tjenestene [209, 210].

B.2 Kvanteteknologi

Ulike typer teknologier utnytter atomiske egenskaper for å oppnå svært nøyaktige PNT-funksjoner.

Atomklokker er et eksempel på en slik teknologi. I dag forskes det på optiske atomklokker som i motsetning til atomklokker som blir brukt i dag, tilbyr en merkbar forbedring i stabilitet [211]. Slike klokker er fortsatt under utvikling, men lettere kommersielle optiske klokker er brukt allerede i dag på navigasjonssatellitter [212].

En kvantetregthetssensor måler endringer i bølgefunksjonen til et metamateriale bestående av veldig kalde atomer som kondenserer sammen til et «superatom» med helt spesielle egenskaper. Prosessen benytter laserkjøling i et vakuumkammer hvor metamaterialet som oppstår holdes sammen i et kraftig magnetfelt. Disse sensorene er overlegne dagens tregthetsnavigasjonssensorer, og vil fungere overalt på og under jorda, under vann, i lufta og i verdensrommet. Systemet er umulig å jamme og er så å si helt stabilt over tid. Sensorene er ekstremt sensitive for akselerasjoner og bevegelser, og er derfor også utsatt for vibrasjoner. I og med at tregthetssensoren er såpass avansert og avhengig av å kjøle atomer nesten helt ned til det absolutte nullpunkt ($-273,15\text{ °C}$), er det vanskelig, å lage et navigasjonssystem av en praktisk størrelse..

Et kvantegravimeter måler gravitasjonen ved å ta tiden på et fallende atom inne i et vakuumkammer. Tyngdekraften varierer over jordkloden basert på landmasser og ulik massedistribusjon i og under jordskorpa, og med gravimeteret kan man følge et gravitasjonskart for å estimere posisjon. Slike systemer er kommersielt tilgjengelige og er et eksempel på en moden kvantebasert sensor. Dette er dog ikke noe man får plass til på for eksempel en drone.

Kvantemagnetometere måler jordens magnetiske felt for å bestemme posisjon med høy grad av nøyaktighet. Slike systemer er svært komplekse og fortsatt under utvikling.

B.3 Sekundærbruk av signaler (signals of opportunity)

Sekundærbruk av signaler (*signals of opportunity* – SoOp) omfatter å benytte signaler til posisjonering som kommer fra kilder med andre formål enn PNT. Slike signaler har potensial til å brukes enten sammen med GNSS eller alene for å estimere en posisjon. Steder der GNSS ikke er tilgjengelig, som mellom høyhus i urbane miljøer, innendørs og i tunneler, er eksempler på bruksområder, i tillegg til GNSS-jammede områder. Det er mange signaler man kan bruke, men felles for alle er at de ikke er ment for PNT og mangler sånn sett noen viktige egenskaper. Dette gjør oppgaven vanskelig og da spesielt med tanke på klokkestabilitet og tidssynkronisering.

Det er mange eksempler i litteraturen hvor man bruker for eksempel digital-tv-signaler (DVB-T) som kringkastes fra basestasjoner på bakken til å estimere egen posisjon [213-215]. Hvis man kjenner posisjonene til basestasjonene, kan man estimere avstandene til dem basert på signalstyrken. Usikkerheten i parameterne som inngår i beregningene gir dog unøyaktige posisjonsestimer sammenlignet med GNSS.

Med inntoget av Starlink og OneWeb har oppmerksomheten flyttet seg fra bakkebaserte signaler til signaler fra verdensrommet. Forskere rundt om i verden forsøker nå å bruke disse globalt tilgjengelige signalene til PNT-estimering. Siden dette er konstellasjoner ment for bredbånds-internett, er også mottaksutstyret utviklet med tanke på det, og er dermed ikke egnet til PNT-estimering. Uten dedikerte mottakere får man ikke dekodet signalene, og man må være kreativ for å finne parametere man kan bruke til å estimere PNT-informasjon. Klokkene om bord er generelt ikke gode nok for å nå opp til GNSS-standard, men på tross av dette er det flere forskningsgrupper som har klart å få til gode posisjonsestimater sammenlignet med for eksempel Iridium STL [216].

B.4 eLoran

Enhanced Long-Range Navigation (eLoran) er den moderniserte versjonen av Loran, og er basert på kraftige radiosignaler fra faste installasjoner. Disse sender synkroniserte signaler med relativt lav frekvens (90–110 kHz) som brukes til å beregne posisjon og tid hos en bruker. Systemet kan gi en posisjonsnøyaktighet på 10–20 meter, men er begrenset til horisontal posisjon og en tidsnøyaktighet på under mikrosekundet sporbar til UTC.

Flere land har tatt i bruk eLoran for å komplementere eksisterende GNSS eller annen satellittbasert PNT [217, 218]. eLoran er mer motstandsdyktig mot elektromagnetiske forstyrrelser på grunn av en lavere frekvens som kan penetrere for eksempel bygninger, tunneler og vann.

eLoran kan baseres på «gammel» Loran-C-infrastruktur utstyrt med Cesium-klokker og andre oppgraderte systemer. Storbritannia benytter den eneste gjenstående Loran-C-stasjonen og bygger seks nye stasjoner for å utvikle sitt eLoran-system. Frankrike og Sør-Korea har også vært involvert i utviklingen av eLoran som en alternativ PNT-løsning. Sør-Korea oppgraderer sin eksisterende Loran-C-infrastruktur som et svar på jamming i sjøområdene.

B.5 White Rabbit

White Rabbit (WR) er navnet på en metode for fiberbasert tidsdistribusjon som bygger på PTP (*precision time protocol*). White Rabbit oppnår tidsbestemmelse med en nøyaktighet på under nanosekundet. Løsningen krever fysiske koblinger mellom nodene. Løsningen benytter åpne protokoller utviklet av Den europeiske organisasjonen for kjernefysisk forskning (CERN). WR er integrert i nasjonale tidsnettverk hos for eksempel Frankrike, Italia og UK, og anbefales i utredningen til Justervesenet og Nkom som en del av en fremtidig nasjonal tidsinfrastruktur i Norge [42].

C Oppsummering av tiltak diskutert av fageksperter

Tiltak	Kommentar	Relevante sårbarhet
Redundans i tidsnettverk	Samtlige aktører med avhengighet til tidssynkronisering diskuterte redundans i egne tidsnettverk.	Avhengighet til GNSS
Kartlegge avhengigheter og sårbarheter	Behovet ble diskutert av flere aktører på grunn av kompleksitet i bruken av tid i det digitale samfunnet og mangel på oversikt om sårbarheter, også for posisjonsbestemmelse.	Mangel på oversikt ved økt digitalisering og automatisering i samfunnet.
Bakkebasert tidsnettverk	Samtlige aktører med behov for tidssynkronisering.	Mangel på alternativ nasjonal tidsreferanse.
Øvelser med bortfall av PNT	Diskutert av flere aktører innenfor både posisjon, navigasjon og tidsbestemmelse.	Avhengighet til GNSS Usikkerhet knyttet til utstyr. Tap av kompetanse ved økt bruk av GNSS teknologi.
Krypterte GNSS-signaler	Diskutert av flere aktører med behov for nøyaktig tidssynkronisering.	Avhengighet til GNSS
Sikret integritet og beskyttelse i utstyr (firewall, anti-jam, maskinlæring)	Diskutert av flere aktører med behov for nøyaktig tidssynkronisering.	Avhengighet til GNSS
Alternative referanserammer	Diskutert av flere aktører med behov for nøyaktig posisjonsbestemmelse	Avhengighet til GNSS
Geografiske distribuerte datasentre	Diskutert av en informant for å øke robusthet i digitale tjenester.	Avhengighet til GNSS

Multi-GNSS-mottakere	Diskutert av flere aktører innenfor både posisjon og tid.	Avhengighet til GNSS
Samarbeid mellom aktører med tidsinfrastruktur	Diskutert av flere aktører med behov for tidssynkronisering.	Avhengighet til GNSS
Overvåking av forstyrrelser	Diskutert av flere aktører med behov for tidssynkronisering.	Avhengighet til GNSS
Bestepraksis og standarder for konfigurasjon	Diskutert av flere aktører innenfor både posisjon og tid.	Mangel på standarder og regelverk knyttet til PNT. Usikkerhet knyttet til utstyr.
Testing av utstyr	Diskutert av flere aktører innenfor både posisjon, navigasjon og tid.	Usikkerhet knyttet til utstyr.
Øke kompetanse på GNSS-uavhengig utstyr	Diskutert av flere aktører innenfor både posisjon, navigasjon, og tid.	Tap av kompetanse ved økt bruk av GNSS teknologi.
Krav og oppmerksomhet hos kommersielle leverandører	Diskutert av flere aktører innen navigasjon og tid.	Mangel på oversikt ved økt digitalisering og automatisering i samfunnet.
GNSS-uavhengige reserveløsninger	Diskutert i sammenheng med posisjons- og navigasjonstjenester.	Sårbare GNSS signaler
PNT integrert i beredskapsplaner	Diskutert av flere aktører innenfor posisjon, tid, og navigasjon.	Sårbare GNSS signaler

Referanser

- [1] Nasjonal sikkerhetsmyndighet, "Risiko 2025. Et sikkert Norge i en usikker verden.," 2025.
- [2] R. Browne, "Russian jammed GPS during major NATO military exercise with US troops," in *CNN*, ed, 2018.
- [3] NTB, "Markant økning i russisk jamming mot Norge," in *VG*, ed, 2024.
- [4] C. Edwards and N. Seidenstein, "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," ISSS, 2025.
- [5] Nasjonal kommunikasjonsmyndighet, "Har avdekket nye alvorlige GPS-forstyrrelser i Øst-Finnmark," ed, 2025.
- [6] Etterretningstjenesten, "Fokus 2025. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.," 2025.
- [7] Etterretningstjenesten, "Fokus 2026," Etterretningstjenesten, Etterretningstjenesten, 2026. [Online]. Available: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus2026_innhold
- [8] Justis- og beredskapsdepartementet, "Meld. St. 9 (2024–2025). Totalberedskapsmeldingen – Forberedt på kriser og krig," 2025. [Online]. Available: <https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20242025/id3082364/>
- [9] S. R. Sellevåg, "Sivil støtte til Forsvaret - en funksjonsbasert tilnærming for modellering av totalforsvarsevne," in "FFI-rapport," Forsvarets Forskningsinstitutt, Kjeller, 22/01207, 2022.
- [10] Menon Economics, "Analyse av satellittbaserte PNT-tjenester," 2026.
- [11] Direktoratet for samfunnssikkerhet og beredskap, "Risikoanalyse av manipulering av satellittbaserte tidssignaler," 2026.
- [12] Justis- og Beredskapsdepartementet, "Totalberedskapsmeldingen," in "Meld. St. 9 (2024-2025)," 2025.
- [13] Justis- og Beredskapsdepartementet, "Samfunnssikkerhet i en usikker verden," in "Meld. St. 5 (2020-2021)," 2020.
- [14] UK Government Office for Science, "Satellite-derived Time and Position: A Study of Critical Dependencies," 2018.
- [15] London Economics, "The economic impact on the UK of a disruption to GNSS," 2023, issue 4.
- [16] Norsk Romsenter, "Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur," in "NRS-Rapport," Oslo, 2013/3, Mars 2013.
- [17] ECORYS, Valdani Vicari & Associati, and FDC, "Impact assessment study on the Use of Galileo for Critical Infrastructures that depend on Satellite Navigation for Timing and Synchronisation," Luxembourg, 2020.
- [18] R. B. Langley, P. J. G. Teunissen, and O. Montenbruck, "Introduction to GNSS," in *Springer Handbook of Global Navigation Satellite Systems*, P. J. G. Teunissen Ed. Australia: Springer International Publishing AG, 2017.
- [19] P. C. Bratheim, S. Himle, K. A. Skaar, O. B. Tangen, and V. Olav, "Referanserammer og transformasjoner," Kartverket, 2023.
- [20] Kartverket, "Information about the Observatory," 2021. [Online]. Available: <https://www.kartverket.no/en/about-kartverket/geodetic-earth-observatory/information-about-the-observatory>.

-
-
- [21] United Nations Geodetic Centre of Excellence, "Hidden Risk. How weaknesses in the global geodesy supply chain could have catastrophic impacts on critical infrastructure and national economies. Background report for decision-makers.," 2024.
- [22] I. H. L. Monsen, "The cyber dimension of space systems - an analysis of offensive cyber operations targeting space infrastructure," in "FFI Rapport," Forsvarets Forskningsinstitutt, Kjeller, 2024.
- [23] B. Ellingsen. "Nye norske satelliter skal gi internettbredbånd til Arktis." Direktoratet for romvirksomhet. <https://www.romsenter.no/aktuelt/asbm> (accessed).
- [24] Direktoratet for romvirksomhet. "Satellittkommunikasjon i Norge." <https://romdirektoratet.no/laer-om-romvirksomhet/satellittkommunikasjon-i-norge> (accessed).
- [25] K. B. Klepper *et al.*, "Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv," Forsvarets Forskningsinstitutt, 23/00879, 2023.
- [26] W. A. Ahmed, L. A. Isiaka, B. Mala, and S. F. Olatoyinbo, "Evolution of GNSS/GPS technology and its applications from ancient times to the present," *Next Research*, vol. 2, no. 3, p. 100387, 2025/09/01/ 2025, doi: <https://doi.org/10.1016/j.nexres.2025.100387>.
- [27] L. Aarønæs, "Nå gir ArcSat-1-satellitten resultater," ed: Forsvarets Forskningsinstitutt, 2025.
- [28] Direktoratet for romvirksomhet. "Dette er Copernicus." <https://romdirektoratet.no/laer-om-romvirksomhet/dette-er-copernicus> (accessed).
- [29] "A Brief History of Atomic Time." National Institute of Standards and Technology. <https://www.nist.gov/atomic-clocks/brief-history-atomic-time> (accessed).
- [30] European Space Agency. "GPS Space Segment." esa navipedia. https://gssc.esa.int/navipedia/index.php?title=GPS_Space_Segment (accessed).
- [31] European Space Agency. "Galileo Space Segment." esa navipedia. https://gssc.esa.int/navipedia/index.php?title=Galileo_Space_Segment (accessed).
- [32] E. Boldbaatar, D. Grant, S. Choy, S. Zaminpardaz, and L. Holden, "Evaluating Optical Clock Performance for GNSS Positioning," *Sensors*, vol. 23, no. 13, p. 5998doi: 10.3390/s23135998.
- [33] E. Batori, N. Almat, C. Affolderbach, and G. Mileti, "GNSS-grade space atomic frequency standards: Current status and ongoing developments," *Advances in Space Research*, vol. 68, no. 12, pp. 4723–4733, 2021/12/15/ 2021, doi: <https://doi.org/10.1016/j.asr.2020.09.012>.
- [34] G. Panfilio and F. Arias, "The Coordinated Universal Time (UTC)," *Metrologia*, vol. 56, no. 4, 2019, doi: 10.1088/1681-7575/ab1e68.
- [35] H. Puttnies, P. Danielis, A. R. Sharif, and D. Timmermann, "Estimators for Time Synchronization - Survey, Analysis, and Outlook," *IoT*, 2020, doi: 10.3390/iot1020023.
- [36] A. Malhotra, I. E. Cohen, and S. Goldberg, "Attacking the Network Time Protocol," presented at the Network and Distributed System Security (NDSS) Symposium, San Diego, USA, 2016.
- [37] A. R. Mahlous, "Quantitative Risk Analysis of Network Time Protocol (NTP) Spoofing Attacks," *IEEE Access*, vol. 12, pp. 164891–164910, 2024, doi: 10.1109/ACCESS.2024.3493759.
- [38] Nasjonal sikkerhetsmyndighet, "Sikring av Network Time Protocol," in "IT-veileder for ugraderte systemer," 2016.

-
-
- [39] B. Moussa, M. Debbabi, and C. Assi, "Security Assessment of Time Synchronization Mechanisms for the Smart Grid," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1952–1973, 2016, doi: 10.1109/comst.2016.2525014.
- [40] BIPM Time Department Data Base, "Table 4. Equipment and source of UTC(k) of the laboratories contributing to TAI in 2025," 2025. [Online]. Available: https://webtai.bipm.org/ftp/pub/tai/annual-reports/bipm-annual-report/table4/table4_2025.pdf
- [41] NTP Pool Project. <https://www.ntppool.org/nb/> (accessed).
- [42] Nasjonal kommunikasjonsmyndighet and Justervesenet, "Kartlegging av behov og utredning av løsninger for etablering av en robust infrastruktur for distribusjon av presist og sporbart klokkesignal," 2025.
- [43] United States Coast Guard Navigation Center. "How AIS Works." <https://www.navcen.uscg.gov/how-ais-works> (accessed).
- [44] *Technical characteristics for VHF automatic system using time division multiple access in the maritime mobile service*, International Telecommunication Union, Geneva, Switzerland, 2026.
- [45] U. Kumar CS, "Synchronisation Methods for the Converging Telecom and Data Centre Infrastructures," presented at the 2023 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), 2023.
- [46] D. Petrov, S. Melnik, and T. Hämäläinen, "Distributed GNSS-Based Time Synchronization and Applications," presented at the 2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Portugal, 2016.
- [47] M. B. 2026. "Kerberos authentication overview in Windows Server." <https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview> (accessed).
- [48] Z. Idrees *et al.*, "IEEE 1588 for Clock Synchronization in Industrial IoT and Related Applications: A Review on Contributing Technologies, Protocols and Enhancement Methodologies," *IEEE Access*, vol. 8, pp. 155660–155678, 2020, doi: 10.1109/access.2020.3013669.
- [49] D. C. Mazur, R. A. Entzminger, J. A. Kay, and P. A. Morell, "Time Synchronization Mechanisms for the Industrial Marketplace," *IEEE Transactions on Industry Applications*, vol. 53, no. 1, pp. 39–46, 2017, doi: 10.1109/tia.2016.2603464.
- [50] S. N. Leksikon. "tungindustri." <https://snl.no/tungindustri> (accessed 2026).
- [51] H. N. Yigitler, B. Badihi, and R. Jantti, "Overview of Time Synchronization for IoT Deployments: Clock Discipline Algorithms and Protocols," *Sensors (Basel)*, vol. 20, no. 20, Oct 20 2020, doi: 10.3390/s20205928.
- [52] B. H. Farsund, T. Søndrol, K. O. Nystuen, L. Hornfelt, S. R. Sellevåg, and V. Pham, "Utvikling av nye IoT-baserte infrastrukturer i samfunnet - utfordringer for nasjonal sikkerhet," in "FFI-Rapport," Forsvarets Forskningsinstitut, Kjeller, 2022.
- [53] A. Zervopoulos *et al.*, "Wireless Sensor Network Synchronization for Precision Agriculture Applications," *Agriculture*, vol. 10, no. 3, 2020, doi: 10.3390/agriculture10030089.
- [54] A. Mahmood, M. I. Ashraf, M. Gidlund, and J. Torsner, "Over-the-Air Time Synchronization for URLCC: Requirements, Challenges and Possible Enablers," in *2018 15th International Symposium on Wireless Communication Systems (ISWCS)*, Lisbon, Portugal, 2018: IEEE, doi: DOI: 10.1109/ISWCS.2018.8491188.
- [55] *Lov om verdipapirhandel (verdipapirhandelloven)*, 2007.

-
-
- [56] Finanstilsynet. "MiFID II / MiFIR." <https://www.finanstilsynet.no/tema/mifid-ii--mifir/> (accessed).
- [57] *Delegert Kommisjonsforordning (EU) 2017/574 av 7. juni 2016 om utfylling av europaparlaments- og rådsdirektiv 2014/65/EU med hensyn til tekniske reguleringsstandarder for klokkes nøyaktighetsgrad*, 2022.
- [58] Kartverket. "Brukerveiledning posisjonstjenester." <https://www.kartverket.no/til-lands/posisjon/brukerveiledning-posisjonstjenester> (accessed).
- [59] H. A. Karimi, 2, Ed. *Advanced Location-Based Technologies and Services*. Boca Raton: CRC Press, 2013.
- [60] IMO, "International Convention for the Safety of Life at Sea (SOLAS), 1974." [Online]. Available: [https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-\(solas\)-1974.aspx](https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas)-1974.aspx).
- [61] *Forskrift om krav til utstyr og installasjon av posisjonsrapporteringsutstyr*, 2010.
- [62] Fiskeridirektoratet. "Posisjonsrapportering (VMS)." <https://www.fiskeridir.no/yrkesfiske/rapportering-pa-havet/posisjonsrapportering> (accessed).
- [63] J. H. Lee, Y. J. Song, I. C. Jeong, and J. H. Won, "Improved position estimation method for locating an encrypted COSPAS-SARSAT beacon," *IET Radar, Sonar & Navigation*, vol. 15, no. 10, pp. 1297–1308, 2021, doi: 10.1049/rsn2.12112.
- [64] N. Kjerstad. "nødpeilesender." Store Norske Leksikon. <https://snl.no/n%C3%B8dpeilesender> (accessed).
- [65] Nasjonal kommunikasjonsmyndighet. "Nødnummer, nødalarm og lokalisering." https://nkom.no/telefoni-og-telefonnummer/nodnummer-nodalarm-og-lokalisering#hvordan_fungerer_aml (accessed).
- [66] DSB. "eCall." <https://www.dsb.no/nodnett/produkter-og-tjenester/driftstjenester/ecall/> (accessed).
- [67] Politiet. "Mobil voldsalarm og omvendt voldsalarm." <https://www.politiet.no/rad/vold-i-nare-relasjoner/voldsalarm-og-omvendt-voldsalarm> (accessed).
- [68] "Retningslinjer til straffegjennomføringsloven," *Straffegjennomføring med elektronisk kontroll*, 2021.
- [69] L. Mæhlum. "landmåling." Store Norske Leksikon. <https://snl.no/landm%C3%A5ling> (accessed).
- [70] L. Mæhlum and E. Ørstavik. "totalstasjon." Store Norske Leksikon. <https://snl.no/totalstasjon> (accessed).
- [71] Avinor, "Kart- og geodatatjenester - krav til innmåling," 2024.
- [72] Bane NOR. Utfesting av linjen [Online] Available: <https://oppslagsverk.banenor.no/jernbanekompetanse/overbygning/sporets-trase/utfesting-av-linjen/>
- [73] *Forskrift om innmåling, dokumentasjon og utlevering av geografisk informasjon om ledninger og annen infrastruktur i grunnen, sjø og vassdrag (ledningsregistreringsforskriften)*, 2022.
- [74] Bergen Kommune, "VA-Norm Krav til innmåling og registrering av vann- og avløpsanlegg," 2019. [Online]. Available: https://va-norm.no/content/uploads/2019/12/Vedlegg-B1-Krav-til-innm%C3%A5ling-og-registrering-av-vann-og-avl%C3%B8p%C3%B8sledninger-12_2019.pdf.
- [75] G. Grzanic, K. Molkersrød, and D. T. Norum, "Overvåking av vassdragsanlegg," Oslo, 2019.

-
- [76] NVE. "Beskrivelse av instrumentering." <https://veiledere.nve.no/fjellskred/overvaking/beskrivelse-av-instrumentering/> (accessed).
- [77] G. Fibbi, M. Del Soldato, and R. Fanti, "Review of the Monitoring Applications Involved in the Underground Storage of Natural Gas and CO₂," *Energies*, vol. 16, no. 1, 2022, doi: 10.3390/en16010012.
- [78] F. Thomas, F. A. Livio, F. Ferrario, M. Pizza, and R. Chalaturnyk, "A Review of Subsidence Monitoring Techniques in Offshore Environments," *Sensors (Basel)*, vol. 24, no. 13, Jun 26 2024, doi: 10.3390/s24134164.
- [79] J. K. Rød and Ø. B. Dick. "geografisk informasjonsvitenskap." Store norske leksikon. https://snl.no/geografisk_informasjonsvitenskap (accessed).
- [80] E. Ørstavik, L. Mæhlum, and J. K. Rød. "geografisk informasjonssystem - GIS." Store norske leksikon. https://snl.no/geografisk_informasjonssystem_-_GIS (accessed).
- [81] M. Apollo *et al.*, "Geodata in Science – a Review of Selected Scientific Fields," *Acta Scientiarum Polonorum Formatio Circumiectus*, vol. 22, no. 2, pp. 17–40, 2023, doi: 10.15576/asp.Fc/2023.22.2.02.
- [82] J. L. Ervik, "KI i Kystverket," in *Status 2025: Kystverket*, 2025, ch. 5.3.
- [83] Kystverket. "Kystverket avvikler DGPS-tjenesten i Norge." <https://www.kystverket.no/nyheter/2024/kystverket-avvikler-dgps-tjenesten-i-norge/> (accessed).
- [84] Avinor, "PBN Transition Plan NORWAY," (EU) 2018/1048 Art. 4, 2023.
- [85] T. Westbrook, "Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe," *Security and Defence Quarterly*, 2024, doi: 10.35467/sdq/178249.
- [86] J. Tryb and J. Hospodka, "GNSS Interference and Security: Impacts on Critical Infrastructure and Mitigation Strategies," in *6th International Conference on Industry 4.0 and Smart Manufacturing*, 2025, vol. 253: Procedia Computer Science, pp. 2635–2644, doi: <https://doi.org/10.1016/j.procs.2025.01.323>.
- [87] T. Westbrook, "The Global Positioning System and Military Jamming: The geographies of electronic warfare," *Journal of Strategic Security*, vol. 12, no. 2, pp. 1–16, 2019, doi: 10.5038/1944-0472.12.2.1720.
- [88] J. Steiner and L. Lukes, "Wide-Area GPS Interference Over Europe From an Unknown Source," presented at the 2022 New Trends in Civil Aviation, 2022.
- [89] H. O. Torgersen and P. Byhring, "Lastebilsjåfører blokkerte GPS-signalene til ambulansehelikopter. Det skjer stadig oftere.," in *Aftenposten*, ed, 2019.
- [90] A. Morrison *et al.*, "Jammertest 2022: Jamming and Spoofing Lessons Learned," presented at the Enc 2023, 2023.
- [91] GPSJAM. <https://gpsjam.org/?lat=56.13946&lon=18.87048&z=3.2&date=2026-03-16> (accessed March 16th 2026).
- [92] F. Dovis, *GNSS interference threats and countermeasures* (The GNSS technology and application series). Boston: Artech House, 2015.
- [93] D. M. Laverty, C. Kelsey, and J. B. O'Raw, "GNSS Time Signal Spoofing Detector for Electrical Substations," *IEEE Transactions on Smart Grid*, vol. 13, no. 2, pp. 1468–1477, 2022, doi: 10.1109/tsg.2021.3122099.
- [94] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and Mitigating Attacks on GPS Devices," *Sensors*, vol. 24, no. 5529, 2025, doi: 10.3390/s24175529.
- [95] H. Zhang, S. Peng, L. Liu, S. Su, and Y. Cao, "Review on GPS spoofing-based time synchronisation attack on power system," *IET Generation, Transmission & Distribution*, vol. 14, no. 20, pp. 4301–4309, 2020, doi: 10.1049/iet-gtd.2020.0253.

-
-
- [96] I. Bowers and H. S. Hiim, "Knock-on Risks to NATO's Space-based War-fighting Capabilities," *Survival*, vol. 67, no. 3, pp. 95–108, 2025, doi: 10.1080/00396338.2025.2508089.
- [97] N. Gerrard *et al.*, "Jammertest: An Open GNSS Interference Test Arena to Accelerate the Development of Resilient GNSS Applications," *Engineering Proceedings*, vol. 126, no. 1, p. 20doi: 10.3390/engproc2026126020.
- [98] P. Marzioli, D. Oltrogge, C. M. Taiatu, M. A. Skinner, and A. Court, "Management of radio-frequency interferences for space traffic management: Current regulations, operations practice, technology mitigation solutions and future trends," *Acta Astronautica*, vol. 225, pp. 1019–1030, 2024/12/01/ 2024, doi: <https://doi.org/10.1016/j.actaastro.2024.10.005>.
- [99] ITU, "Summary of decisions of the 96th meeting of the radio regulations board," in "Radio Regulations Board," Geneva, 2024.
- [100] S. Nyhamn, A. Sauter, and G. Pettersen, "Rapport etter Jammetest Andøya 2023," in "Kunnskapsbygging GNSS interferens Kystverket," 2, 2024.
- [101] European Space Policy Institute (ESPI), "Espir Report 84 - The war in Ukraine from a space cybersecurity perspective," in "ESPI Rerport," European Space Policy Institute (ESPI), Vienna, 2022.
- [102] Nasjonal kommunikasjonsmyndighet, "Risiko- og sårbarhetsanalyse for ekomsektoren," 2024.
- [103] C. Poirier, "Hacking the Cosmos: Cyber operations against the space sector. A case study from the war in Ukraine.," Center for Security Studies (CSS), ETH Zürich, Zürich, 2024.
- [104] R. Thummala, "Space Worms: On the threat of cyber-asat weaponry to satellite constellations," Cyber Security and Operations, The Pennsylvania State University, 2023.
- [105] J. Yao, M. A. Lombardi, A. N. Novick, B. Patla, J. A. Sherman, and V. Zhang, "The effects of the January 2016 UTC offset anomaly on GPS-controlleg clocks monitored at NIST," in *48th Annual Precise Time and Time Interval Systems and Applications Meeting*, 2017, doi: DOI:10.33012/2017.14989.
- [106] G. Pettersen, O. S. Hareide, S. Nyhamn, and A. Sauter, "2.2 Hvordan beskytte kysten mot hybrid krigføring," in *Status 2025: Kystverket*, 2025.
- [107] V. Kovarik, "Threats to Satellite Systems in the Earth Orbit," *Advances in Military Technology*, vol. 19, no. 1, pp. 25–40, 2024, doi: 10.3849/aimt.01853.
- [108] J. Sankaran, "Russian Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace superiority," in *Arms Control Association*, ed, 2022.
- [109] U.S Department of Defense, "Military and security developments involving The People's Republic of China," in "Annual Report to Congress," 2024.
- [110] C. Swope, K. A. Bingen, M. Young, and K. Lafave, "Space Threat Assessment 2025," Center for Strategic and International Studies, 2025.
- [111] A. Bos, M. Snijders, A. Zevenbergen, K. Drost, H. Zelle, and B. van der Hoeven, "Robustness Levels of Critical Infrastructures Against Global Navigation Satellite System Signal Disturbances," presented at the Eng 2023, 2023.
- [112] J. C. Bergaust and S. R. Sellevåg, "Improved conceptualising of hybrid interference below the threshold of armed conflict," *European Security*, vol. 33, no. 2, pp. 169–195, 2024/04/02 2024, doi: 10.1080/09662839.2023.2267478.
- [113] T. Westbrook, "Radiofrequency Interference Strategies Targeting Marine Navigation Systems: Political Motives and Consequences," *Journal on Baltic Security*, vol. 9, no. 1, pp. 69–97, 2023.

-
- [114] M. Czajkowski, "Anti-Satellite Weapons – Current Status," *Roczniki Nauk Społecznych*, vol. 52, no. 4, pp. 183–201, 12/23 2024, doi: 10.18290/rms2024.0043.
- [115] M. W. Bockmann. (2019) Seized UK tanker likely 'spoofed' by Iran. *Lloyd's List*. Available: <https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran>
- [116] M. Harris. (2021) Phantom Warships Are Courting Chaos in Conflict Zones. *Wired*. Available: <https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/>
- [117] H. Lied, "Norske marineskip ble manipulert inn i russisk farvann," in *NRKBeta*, ed, 2021.
- [118] A. Edvardsen, "Ingen nye tegn til GPS-forstyrrelser i Barentshavet," in *High North News*, ed, 2025.
- [119] A. Walsh, "Sweden accuses Russia og GPS jamming over Baltic Sea," in *BBC*, ed, 2025.
- [120] L. Höller, "Researchers home in on origins of Russia's Baltic GPS jamming," in *Defense News*, ed, 2025.
- [121] The Economist, "Who is jamming airliner's GPS in the Baltic?," in *The Economist*, ed, 2024.
- [122] K. A. Bingen, "Extending the Battlespace to Space," in *War and the Modern Battlefield. Insights from Ukraine and the Middle East*, S. G. Jones and S. P. Daniels Eds.: Center for Strategic & International Studies, 2025, ch. 8.
- [123] S. Waterman, "GPS Jamming Extends to Low-Earth Orbit as Pentagon Races to Bolster Constellation," in *Air & Space Forces Magazine*, ed, 2025.
- [124] Direktoratet for samfunnssikkerhet og beredskap, "Analyser av krisescenarioer 2019," 2019.
- [125] V. E. Elfsnes, "Elektronikken på jorda blir slått ut av solstormer på sola," ed, 2025.
- [126] T. Aven, "Reflections on the Use of Conceptual Research in Risk Analysis," *Risk Analysis*, vol. 38, no. 11, pp. 2415–2423, 2018/11/01 2018, doi: <https://doi.org/10.1111/risa.13139>.
- [127] T. Aven *et al.*, "Society for Risk Analysis Glossary," 2018.
- [128] S. R. Sellevåg, "Totalforsvarets avhengighet til satellittbasert posisjon, navigasjon og tid - vedlegg til FFI-rapport 26/013 (BEGRENSET)," Forsvarets Forskningsinstitutt, Kjeller, 2026.
- [129] Justis- og Beredskapsdepartementet, "Nå er det alvor. Rustet for en usikker fremtid.," in "NOU 2023 : 17," 2023.
- [130] NATO. "Energy Security." NATO. <https://www.nato.int/en/what-we-do/wider-activities/energy-security> (accessed).
- [131] *Veiledning til kraftberedskapsforskriften*, NVE, NVE Digital Veileder, 2024.
- [132] *Forskrift om sikkerhet og beredskap i kraftforsyningen*, 2012.
- [133] M. Røyksund and A.-K. Valdal, "Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning," in "NVE Ekstern Rapport," 2020.
- [134] Statnett, "NVF 2024 Nasjonal veileder for funksjonskrav i kraftsystemet," 2024.
- [135] Statnett, "Strategisk plan teknologi," Oslo, 2025.
- [136] D. Shepard, T. E. Humphreys, and A. A. Fansler. (2012) Going Up Against Time. *GPS World*.
- [137] T. Etchells, K. L. Aplin, L. Berthoud, A. Kalavana, and A. Larkins, "Extreme Space Weather Impacts on GNSS Timing Signals for Electricity Grid Management," *Space Weather*, vol. 22, no. 10, 2024, doi: 10.1029/2023sw003770.
- [138] (2024). *Prop. 87 S (2023-2024) - Forsvarsløftet - For Norges Trygghet*. [Online] Available:

-
-
- <https://www.regjeringen.no/contentassets/27e00e5acc014c5ba741aacff235d99/no/pdfs/prp202320240087000dddpdfs.pdf>
- [139] G. A. Birkemo, L. Hübert, and T. Grunnan, "Nasjonal forsyningssikkerhet i krise og krig - sårbarheter, konsekvenser og tiltak for mat- og drivstofforsyningen," Forsvarets Forskningsinstitutt, Kjeller, 2026.
 - [140] R. Stoop, I. Patrahau, and C. Cassidy, "Securing European Military Fuels in a Tense Security Environment - Supply, Distribution and Storage," The Hague Centre for Strategic Studies, 2025.
 - [141] Standards Norway. "NORSOK standards." <https://standard.no/en/sectors/petroleum/norsok-standards/> (accessed.
 - [142] L. J. Gressgård, K. Melberg, M. Risdal, J. T. Selvik, and R. Ø. Skotnes, "Digitalisering i petroleumsnæringen," Petroleumstilsynet, 2018.
 - [143] G. K. Hanssen, T. Onshus, M. G. Jaatun, T. Myklebust, M. Ottermo, and M. A. Lundteigen, "Premisser for digitalisering og integrasjon IT-OT," SINTEF, 2021.
 - [144] Nasjonal kommunikasjonsmyndighet, "EkomROS 2025," 2025. [Online]. Available: <https://nkom.no/rapporter-og-dokumenter/ekomros-2025>
 - [145] Telenor, "Digital sikkerhet 2023," 2023. [Online]. Available: https://www.telenor.no/binaries/om/digital-sikkerhet/2023/Digital_sikkerhet_2023.pdf
 - [146] O. P. Galaasen, "Slik skal Norge sikre trygg vannforsyning i fremtiden," in *VA nytt*, ed, 2025.
 - [147] M. G. Jaatun, J. Røstum, and S. Petersen, "Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer," in "Norsk Vann Rapport," 2013.
 - [148] A. K. Desjardins, M. Beheshti, and S. Særgrov, "Fremtidens vann- og avløpssystem," in "Norsk Vann Rapport," Norsk Vann, 2023.
 - [149] C. F. Nordheim, M. Steinberg, and T. M. Lyngstad, "Oppdrag fra Mattilsynet - Rapportering av data for vannforsyningssystemer i Norge for 2023," Folkehelseinstituttet, 2024.
 - [150] Schneider Electric, "System Time Stamping User Guide," in "Original Instructions," France, 2022.
 - [151] S. Bruaset and J. Røstum, in "Digital Water City in Norway," 2022.
 - [152] Norges Bank, "Det norske finansielle systemet," 2025.
 - [153] Norges Bank, "Finansiell infrastruktur 2025," Norges Bank, 2025. [Online]. Available: <https://www.norges-bank.no/aktuelt/publikasjoner/Finansiell-infrastruktur---rapport/finansiell-infrastruktur-2025/>
 - [154] E. Skjelland, S. Glærum, T. Nyhamar, and C. Sendstad, "Forsvarsanalysen 2025," in "FFI-Rapport," Forsvarets Forskningsinstitutt, Kjeller, 2025.
 - [155] *Forskrift om navigasjon og navigasjonshjelpemidler for skip og flyttbare innretninger*, 2014.
 - [156] N. Kjerstad. "ECDIS (kartplotter)." Store Norske Leksikon. https://snl.no/ECDIS_-_kartplotter (accessed.
 - [157] RIN GNSS Interference Working Group, "Impacts of GNSS Interference on Maritime Safety - A special report by the RIN Maritime GNSS Interference Working Group," Royal Insitute of Navigation, 2026.
 - [158] *REVISED MARITIME POLICY AND REQUIREMENTS FOR A FUTURE GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS)*, 2002.
 - [159] N. Kjerstad. "AIS." Store Norske Leksikon. <https://snl.no/AIS> (accessed.
 - [160] N. Kjerstad. "radiofyr." Store Norske Leksikon. <https://snl.no/radiofyr> (accessed.

-
-
- [161] J. Xiao, Y. Li, C. Zhang, and Z. Zhang, "INS/GPS Integrated Navigation for Unmanned Ships Based on EEMD Noise Reduction and SSA-ELM," *Journal of Marine Science and Engineering*, vol. 10, no. 11, 2022, doi: 10.3390/jmse10111733.
- [162] J. Wang, Y. Xiao, T. Li, and C. L. P. Chen, "A Jamming Aware Artificial Potential Field Method to Counter GPS Jamming for Unmanned Surface Ship Path Planning," *IEEE Systems Journal*, vol. 17, no. 3, pp. 4555–4566, 2023, doi: 10.1109/jsyst.2023.3237613.
- [163] S. G. Kvarven, "GPS-jamming: Rammer nesten 1.000 skip daglig," in *Finansavisen*, ed, 2025.
- [164] L. A. LaRocco, "Strait of Hormuz GPS jamming remains major security issue, tanker CEO says," in *CNBC*, ed, 2025.
- [165] G. Howard, "Qatar lifts some navigation restrictions as GPS fault continues," in *Seatrade Maritime News*, ed, 2025.
- [166] Lloyd's List, "Qatar halts all navigation due to GPS fault," in *Lloyd's List*, ed, 2025.
- [167] A. Skifjeld and E. Molde, "Norske satellitter skal avdekke ulovlig fiske," in *NRK*, ed, 2022.
- [168] T. Jonassen, "Bekymret for mulig skyggeflåte ved Svalbard," in *NRK*, ed, 2025.
- [169] K. H. Honningsøy, "Skal ha funnet mystiske "mørke skip" for Nord Stream-eksplosjonene," in *NRK*, ed, 2022.
- [170] B. M. Pettersen *et al.*, "Spionskipene," in *NRK*, ed, 2024.
- [171] Nærings- og fiskeridepartementet, "Lansert nytt verktøy i arbeidet mot fiskerikriminalitet," Regjeringen, Ed., ed, 2024.
- [172] M. Stróżyna, "Maritime Anomalies Detection," in *Data Analysis in the Maritime Domain*, M. Stróżyna, W. Abramowicz, K. Weceł, D. Filipiak, and J. Malyszko Eds. Poznań: Poznań University of Economics and Business, 2022, ch. 6.
- [173] "Skyggeflåten utfordrer sikkerheten i europeiske farvann - Norge tar ansvar," in *Kystverket*, ed, 2025.
- [174] FFI, "NorSat-3 - Skipsovervåking med navigasjonsradardetektor," in "Fakta," Forsvarets Forskningsinstitutt, 2021.
- [175] "Ny satellitt skal styrke norsk havovervåking," in *FFI*, ed, 2025.
- [176] Statens vegvesen, "ITS-strategi for Statens vegvesen 2018-2023. Et vegkart mot fremtidens transportsystem.," Vegdirektoratet, 2018.
- [177] S. Raza, A. Al-Kaisy, R. Teixeira, and B. Meyer, "The Role of GNSS-RTN in Transportation Applications," *Encyclopedia*, vol. 2, no. 3, pp. 1237–1249doi: 10.3390/encyclopedia2030083.
- [178] Riksrevisjonen, "Dokument 3:11 (2024-2025) - Totalforsvaret i sikkerhetspolitisk krise og krig," 2025.
- [179] Bane NOR, "Togradio." [Online]. Available: <https://www.banenor.no/for-deg-i-bransjen/togselskap/togradio/>.
- [180] Jernbanedirektoratet, "KVU FRMCS - Fremtidig togkommunikasjonssystem for jernbane," 2023. [Online]. Available: <https://www.jernbanedirektoratet.no/utredninger/kvu-frmcs-fremtidig-togkommunikasjonssystem-for-jernbane/>
- [181] Avinor, "Ny teknologi gjør luftrommet tryggere i Norge," ed: NTB Kommunikasjon, 2023.
- [182] Luftfartstilsynet, "Navigasjonsstrategi for luftfart i Norge," 2020.
- [183] Avinor. "Digitale tårn." <https://om.avinor.no/flysikring/digitale-tarn/> (accessed.

-
-
- [184] M. Felux, P. Fol, B. Figuet, M. Waltert, and X. Olive, "Impacts of Global Navigation Satellite System Jamming on Aviation," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, 07/29 2024, doi: 10.33012/navi.657.
- [185] I. Prezelj and J. Juvan, "Global navigation satellite systems as critical infrastructure: A cross-sectoral impact assessment of service interruptions in Europe," *Progress in Disaster Science*, vol. 29, p. 100504, 2026/01/01/ 2026, doi: <https://doi.org/10.1016/j.pdisas.2025.100504>.
- [186] V. Renaudin, M. I. Sayyaf, F. Le Bourhis, and M. Ortiz, "GNSS Positioning Under Threat: The Rising Risk to Existing Systems and The Role of Alternative Indoor and Seamless Navigation Technologies," *IEEE Journal of Indoor and Seamless Positioning and Navigation*, vol. 3, pp. 246–259, 2025, doi: 10.1109/jispin.2025.3629705.
- [187] Samferdselsdepartementet and Forsvarsdepartementet, "Norsk Luftstrømsstrategi," 2021. [Online]. Available: <https://www.regjeringen.no/contentassets/dbfc0a975c774e4186d6985ea35da66f/no/pdfs/norsk-luftstromstrategi.pdf>
- [188] M. Hussong, E. Ghizzo, C. Milner, and A. Garcia-Pena, "GNSS performance degradation under meaconing in civil aviation: pseudorange and position models," *GPS Solutions*, vol. 29, no. 3, 2025, doi: 10.1007/s10291-024-01804-6.
- [189] C. Bessing, "Det blinker og uler i cockpiten: Villedende GPS-signaler truer flysikkerheten," in *Teknisk Ukeblad*, ed, 2025.
- [190] ASKO Oslofjord AS. [Online]. Available: https://www.visbrosjyre.no/AskO_Oslofjord/WebView/?utm_term=ASKO%20OSLOFJORD%20AS%20kundeside&utm_source=eMarketeer&utm_campaign=ASKO%20OSLOFJORD%20AS%20forside&utm_medium=referral&utm_content=ASKO%20OSLOFJORD%20AS%20hovedside&utm_em_source=3032b469bdb11b739e634e2cfe9177662f29938f76e3ddc65e385e8b97d593642ba0.
- [191] Landbruks- og matdepartementet, "Endringer i statsbudsjettet 2024 under Landbruks- og matdepartementet (Jordbruksoppgjøret 2025)," in "Prop. 149 S (2024-2025)," 2025.
- [192] V. Lillestrøm, M. Haddara, and M. Langseth, "Unlocking the Potentials of IoT Adoption in Agriculture: Insights from Norwegian Farmers," *Procedia Computer Science*, vol. 239, pp. 1015–1026, 2024/01/01/ 2024, doi: <https://doi.org/10.1016/j.procs.2024.06.265>.
- [193] B. Ellingsen, "Sikrere innflygning for politiets helikoptre," in *Direktoratet for romvirksomhet*, ed, 2024.
- [194] P. E. Dalløkken and E. H. Urke, "Norsk Luftambulanses lavtflygning er utenkelig i mange andre land," in *Teknisk Ukeblad*, ed, 2023.
- [195] R. M. W. Sæther, "GPS-forstyrrelser skaper hodebry for luftambulansen," in *Norsk Luftambulans Stiftelse*, ed, 2025.
- [196] Digitaliserings- og Forvaltningsdepartementet and Justis- og Beredskapsdepartementet, "Regjeringen vil bruke moderne 5G-teknologi for Norges nye nødnett," ed: Regjeringen, 2025.
- [197] T. F. Kristensen, "Luftambulansen utsatt for massiv GPS-jamming: - Tyder på at det stammer fra Russland," in *NRK*, ed, 2022.
- [198] Forsvarsdepartementet, "Dronestrategi for forsvarssektoren," Regjeringen, 2025.
- [199] J. J. R. Critchley-Marrows and Q. Verspieren, "Ensuring PNT resilience in a time of navigation uncertainty," *Space Policy*, vol. 72, 2025, doi: 10.1016/j.spacepol.2024.101665.

-
-
- [200] Å. Davidsson, B. Johansson, S. Nilsson, S. Bergström, and M. Alexandersson, "Metodstöd för analys av GNSS-beroenden. Delområde: Tid och frekvens," Totalförsvarets forskningsinstitut, 2025.
- [201] DHS, "Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture," The Department of Homeland Security (DHS) Science and Technology Directorate (S&T), 2022.
- [202] European Commission, "European Radio Navigation Plan 2023," 2023.
- [203] I. a. T. Department for Science. "Positioning, Navigation and Timing: Overview." <https://www.gov.uk/guidance/positioning-navigation-and-timing-overview> (accessed.
- [204] The Economist, "America is upgrading GPS to catch up with rivals," in *The Economist*, ed, 2025.
- [205] The Economist. (2025) Can China jam your GPS? *The Economist*. Available: <https://www.economist.com/international/2025/05/22/can-china-jam-your-gps>
- [206] S. R. Sellevåg and K. B. Klepper, "Styrket sikkerhet og beredskap i kraftforsyningen - tiltak og prioriteringer," in "FFI-Rapport," Forsvarets Forskningsinstitut, Kjeller, 2025.
- [207] Samferdselsdepartementet, "På rett sted til rett tid: Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse," N-0570 B, 2018.
- [208] European Union Agency for the Space Programme, "EUSPA EO and GNSS Market Report," 2024, issue 2.
- [209] M. Gala *et al.*, "The rise of LEO PNT - GPS World," ed, 2026.
- [210] E. Rubinov, "State of Market Report, Low Earth Orbit Positioning Navigation and Timing - 2024 Edition," FrontierSI, 2024 2024. Accessed: 2026-01-28 10:11:38.
- [211] J. Chu, "MIT physicists improve the precision of atomic clocks," in *MIT News*, ed, 2025.
- [212] NIST. "Optical Clocks: The Future of Time." <https://www.nist.gov/atomic-clocks/how-atomic-clocks-work/optical-clocks-future-time> (accessed.
- [213] R. Kapoor, S. Ramasamy, A. Gardi, and R. Sabatini, "UAV Navigation using Signals of Opportunity in Urban Environments: A Review," *Energy Procedia*, vol. 110, pp. 377–383, 2017/03/01/ 2017, doi: <https://doi.org/10.1016/j.egypro.2017.03.156>.
- [214] J. Rydell, A. Hellander, J. Eek, and G. Hendeby, "Localization Using DVB-T Signals: Experimental Insights and Validation," in *2025 28th International Conference on Information Fusion (FUSION)*, 7–11 July 2025 2025, pp. 1–8, doi: 10.23919/FUSION65864.2025.11124006.
- [215] J. Huang, L. Lo Presti, and R. Garelli, "Digital Video Broadcast-Terrestrial (DVB-T) Single Frequency Networks Positioning in Dynamic Scenarios," *Sensors*, vol. 13, no. 8, pp. 10191–10218doi: 10.3390/s130810191.
- [216] W. J. Morrison and T. E. Humphreys, "Development of a Real-Time Software-Defined Receiver for Broadband LEO PNT," (in en).
- [217] T. Cozzens, "UK invests in satellite timing infrastructure to strengthen national PNT resilience," in *GPS World*, ed, 2026.
- [218] D. Goward, "South Korea partners with broadcaster on eLoran and 10-cm GPS," in *GPS World*, ed, 2020.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan. Med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål

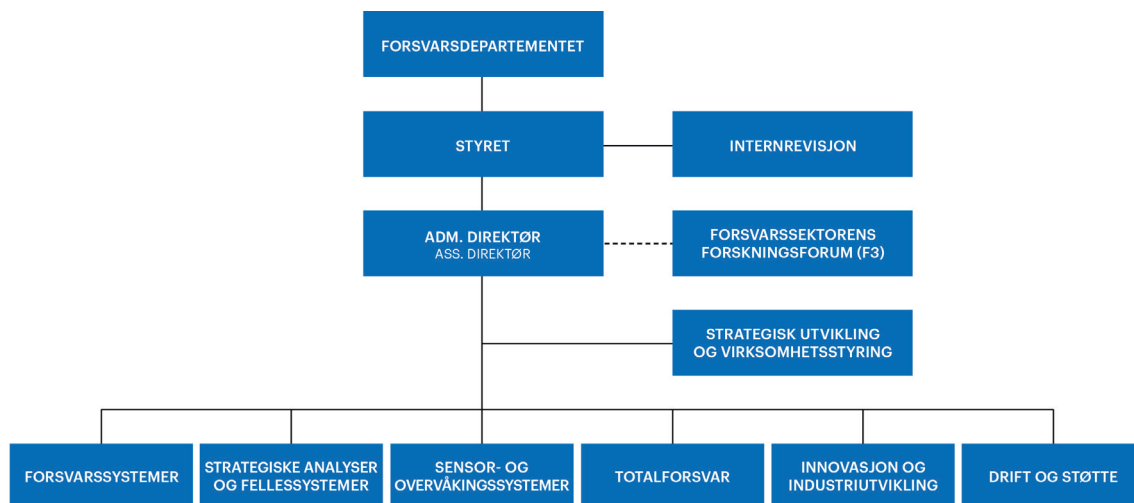
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier

Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en